НАЦІОНАЛЬНА АКАДЕМІЯ УПРАВЛІННЯ

Ковтунець В.В. Нестеренко О.В. Савенков О.І.

БЕЗПЕКА СИСТЕМ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ

Навчальний посібник

Київ – 2016

ББК 004
УДК 681.324
К 56
Рекомендовано до видання вченою радою Національної академії управління (Протокол № 4 від 31 серпня 2016 р.)

Рецензенти:

Д.В. Ланде, доктор технічних наук, старший науковий співробітник, Інститут проблем реєстрації інформації НАН України

О.К. Лопатін, доктор фізико-математичних наук, професор, Національна академія управління

О.А. Курченко, кандидат технічних наук, доцент, Навчально-науковий інститут захисту інформації Державного університету телекомунікацій

К 56 **Ковтунець В.В., Нестеренко О.В., Савенков О.І.**
Безпека систем підтримки прийняття рішень: Навч. посібник. – К. : Національна академія управління, 2016. – 190 с.

ISBN 978-617-7386-00-0

Цей навчальний посібник містить систематизоване викладення навчальної дисципліни «Криптологія та захист інформації в автоматизованих системах» для студентів, що навчаються на бакалаврських програмах за спеціальністю «Комп' ютерні науки та інформаційні технології», магістерських програмах за спеціальностями «Системний аналіз» та «Системи і методи прийняття рішень». Крім того, навчальний посібник може використовуватись студентами ВНЗ, що вивчають дисципліни з економіки, бізнесу, управління та адміністрування.

Безпека систем підтримки прийняття рішень, які є перспективним напрямом автоматизації управлінської праці, набуває усе більшої важливості. Враховуючи сучасні можливості інформаційно-комунікаційних технологій та тенденції збільшення кількості загроз інформаційній та кібербезпеці, питання захисту інформації в СППР набувають усе більшої актуальності. У посібнику викладено основні відомості про напрями та рівні забезпечення безпеки, основні заходи та засоби захисту інформації в СППР, методи побудови захищених СППР, а також особливості архітектури такого роду систем.

Крім студентів та викладачів це видання може бути корисним й для керівників і фахівців фінансово-економічної сфери, державних службовців, а також для науковців, яких цікавлять проблеми безпеки інформаційних систем.

ISBN 978-617-7386-00-0
ББК 004
УДК 681.324

ЗМІСТ

ПЕРЕЛІК РИСУНКІВ

ПЕРЕЛІК СКОРОЧЕНЬ

ТСВ	- Trusted Computing Base (довірча обчислювальна база)
АІС	- автоматизована інформаційна система;
АВПЗ	- антивірусний програмний засіб;
АРМ	- автоматизоване робоче місце;
БД	- база даних;
БЗ	- база знань;
ЕОТ	- електронна обчислювальна техніка;
ЕЦП	- електронний цифровий підпис;
ІзОД	- інформація з обмеженим доступом:
ІТ	- інформаційні технології;
КЗЗ	- комплекс засобів захисту;
КСЗІ	- комплексна система захисту інформації;
ЛОМ	- локальна обчислювальна мережа;
НСД	- несанкціонований доступ;
ПБ	- політика безпеки;
ПЕМВН	- витік по каналах побічних електромагнітних випроміню-вань і наведень;
ПЗ	- програмне забезпечення;
СППР	- система підтримки прийняття рішень;
ТЗІ	- технічний захист інформації;
ОПР	- особа, що приймає рішення;
СКБД	- система керування базою даних;
ФПЗ	- функціональний профіль захищеності.

ВСТУП

Сучасний етап розвитку суспільства міцно пов'язаний із стрімким технологічним зростанням та розбудовою ***інформаційного суспільства,*** у якому завдяки широкому використанню ***інформаційно-комунікаційних технологій*** суттєво збільшується інтенсивність інформаційного обміну, а основним типом діяльності стає обробка інформації та генерування нового знання.

Завдяки сучасним темпам розвитку інформаційних технологій усе більш широке використання у різних сферах діяльності знаходять та постійно вдосконалюються ***системи підтримки прийняття рішень*** (СППР). Враховуючи існуючи можливості застосувань, інтерес до СППР як до перспективного напряму забезпечення підтримки прийняття рішень і потужного інструментарію підвищення ефективності праці у сфері управління безперервно зростає.

Вказані чинники стають визначальними у розвитку економіки, науки, освіти. Водночас обумовлена цими обставинами відкритість діяльності підприємств та організацій, взаємозалежність технологій та сфер діяльності веде до потенційної уразливості, техногенної небезпеки. Протягом останніх років спостерігається стійка тенденція до різкого збільшення загроз з точки зору кількості спроб зловмисного втручання в роботу автоматизованих інформаційних систем та несанкціонованого доступу до інформації, яка в них циркулює, а також появи нових методів та алгоритмів щодо їх здійснення. У кіберзлочинців особливо зростає увага до систем класу СППР, адже в них зосереджена особо цінна аналітична та консолідована інформація. Крім того, зацікавленість порушників підігрівається й наявністю в цих системах передових математичних моделей і методів, унікальних алгоритмів та програмних засобів. У таких умовах ці системи повинні вміти протистояти різноманітним атакам, як зовнішнім, так і внутрішнім, як атакам локальним, так і глобально скоординованим, а ***інформаційна та кібербезпека*** подібних аналітичних систем стає одним з найважливіших аспектів інтегральної безпеки, не лише персонально особи, що приймає рішення або корпоративної, а й національної.

Проблемам забезпечення безпеки інформації, захисту інформаційного простору від небажаного інформаційного впливу, забезпеченню без-

печного функціонування інформаційно-телекомунікаційних систем та захисту інформації, що циркулює в них, приділяється серйозна увага як держаних органів, так і науковців і фахівців, завдяки чому на цей час напрацьовано чимало теоретичних робіт та отримані значні практичні результати.

Виходячи з викладеного, а також враховуючи, що підготовка фахівця за спеціальностями «Комп'ютерні науки та інформаційні технології», «Системний аналіз» є дуже важливою, роль та значення дисциплін, пов'язаних з питаннями захисту інформації в автоматизованих системах серед інших дисциплін, що вивчаються, набуває також виняткового значення. При цьому вбачається, що за вказаними напрямками підготовки базою для вивчення цих дисциплін мають стати власне ті особливості, які притаманні саме системам підтримки прийняття рішень, а основними задачами, що стоять перед студентом є засвоєння основ аналізу загроз процесам прийняття рішень у різних предметних областях, розуміння необхідності застосування моделей безпеки та їх вибору з урахуванням особливостей представлення та організації даних та знань, отримання навичок з побудови захищених СППР, уявлень щодо архітектур такого роду систем, особливостей інтерфейсу користувача. Для закріплення практичних навичок необхідно ознайомитись з прикладами реалізації необхідної безпеки СППР в різних сферах.

Композиція посібника та викладення навчального матеріалу в основному зорієнтоване на кількість годин у навчальному плані, відведених на дисципліну для аудиторних занять – один підрозділ (іноді два) на лекцію. Питання, тести, задачі, завдання відповідають практичним заняттям, а також кількості годин у навчальному плані, відведених для самостійної роботи студентів. Вони спрямовані на активізацію пізнавальної діяльності, самостійної творчої праці та отримання вміння розв'язувати задачі.

Важливою особливістю завдань є те, що вони мають не локальний характер, а спрямовані на комплексне завдання поступового проектування студентом упродовж курсу власної захищеної СППР, функціональне призначення якої він отримує як завдання до курсового проекту, дипломного проектування або вибирає на власний розсуд.

У тексті посібника застосовуються піктограми, які полегшують орієнтацію та пошук певних структурних його елементів, а саме:

 – основні визначення;

 – приклади;

 – контрольні запитання та завдання;

 – заслуговує на окрему увагу.

Для полегшення користування посібником наприкінці наведений предметний покажчик (термінів, основних визначень та понять, на яких базується викладення матеріалу).

Автори висловлюють подяку Т.В. Шулькевич за допомогу у підготовці рукопису посібника.

Фотоматеріали, довідкова інформація отримані з різних відкритих джерел Інтернету, яким автори висловлюють свою повагу і шанування.

1. ІНФОРМАЦІЙНА ТА КІБЕРБЕЗПЕКА

1.1. ПРЕДМЕТ БЕЗПЕКИ ІНФОРМАЦІЇ

Основні поняття.
Визначення та загальні властивості інформації.
Поняття інформаційної безпеки, кібербезпеки та захисту інформації.
Основні технології кібербезпеки.

1.1.1. Основні поняття

Великою звитягою розвитку цивілізації стало здобуття людиною права на інформацію. У резолюції Генеральної Асамблеї ООН від 10.12.1948 р. сказано, що «свобода інформації є основним правом людини і являє собою критерій усіх видів свободи». Постіндустріальне суспільство, у якому ми з вами живемо, вважає найвищою цінністю саме інформацію, яку, водночас, потрібно зберігати не менш ретельно, ніж золотий запас. Ця діалектика вільного поширення інформації та одночасного обмеження доступу до неї власне й є причиною тієї великої уваги, що приділяється проблематиці безпеки інформації.

Проблеми і задачі забезпечення безпеки інформації, схоронності інформаційних ресурсів, охорони різного роду таємниць виникли й вирішувалися задовго до комп'ютерної ери. Ще у середні віки великий мислитель Леонардо да Вінчі казав, що «очі та вуха, охочі до чужих секретів, завжди знайдуться». Не буде перебільшенням зазначити, що уся історія людства пов'язана з ***інформаційними злочинами***, тобто фактами порушення ***безпеки інформації***, які зводяться, взагалі кажучи, до викрадання або знищення інформації. Такі злочини часто-густо мали суттєві наслідки не лише для окремих осіб, а й для держав і навіть для розвитку цивілізації.

У наші часи щодалі все частіше зустрічається у різних сферах діяльності словосполучення «інформаційна безпека», причому у різних контекстах може мати різний зміст. Переважно воно використовується у ши-

рокому значенні, як стан захищеності національних інтересів в інформаційній сфері, обумовлених сукупністю збалансованих інтересів особистості, суспільства й держави. Під інформаційною безпекою (ІБ) також розуміється захист інтересів суб'єктів інформаційних відносин та інфраструктури, що підтримує їх взаємодію.

Інформаційний злочин *(Information crime)* – Навмисні дії, спрямовані на розкрадання або руйнування інформації в інформаційних системах, які виходять з корисливих або хуліганських спонукань[1].

Безпека інформації *(Information security)* – Стан інформації, за котрого виключаються випадкові або навмисні несанкціоновані впливи на інформацію або несанкціоноване її отримання.

Інформаційна безпека *(Information security)* – Стан захищеності інформаційного середовища суспільства, що забезпечує його формування, використання та розвиток в інтересах громадян, організацій і держави.

Інформаційна безпека – Стан захищеності суб'єктів інформаційних відносин та інфраструктури, що підтримує їх взаємодію від випадкових або навмисних впливів природного або штучного характеру, які можуть нанести збитки власникам або користувачам інформації та підтримуючої інфраструктури.

З поняттям інформаційної безпеки безпосередньо пов'язані й поняття ***інформаційного середовища*** та ***інформаційного простору***, які між собою суттєво зближені.

Таким чином, розглядаючи з інформаційної точки зору середовище підприємства (установи, організації), де у суспільстві переважно реалізуються інформаційні відношення, його можна структурувати на безпосередньо інформаційний простір галузі, у якій проводить свою діяльність підприємство та яке складається з інформаційних середовищ власне підприємств та корпорацій, національний інформаційний простір, і навіть глобальний інформаційний простір (рис. 1.1).

Інформаційний простір *(Information space)* – Середовище, де здійснюється формування, збір, зберігання та розповсюдження інформації.

[1] Під інформаційною системою тут будемо розуміти будь-яку сукупність інформаційних відношень, не обов'язково автоматизованих (паперовий документообіг, бібліотеки, поштове листування, тощо)

Інформаційне середовище *(Information environment)* – Сукупність засобів зберігання, обробки і передачі інформації, а також політичні, економічні і культурні умови реалізації інформаційних процесів.

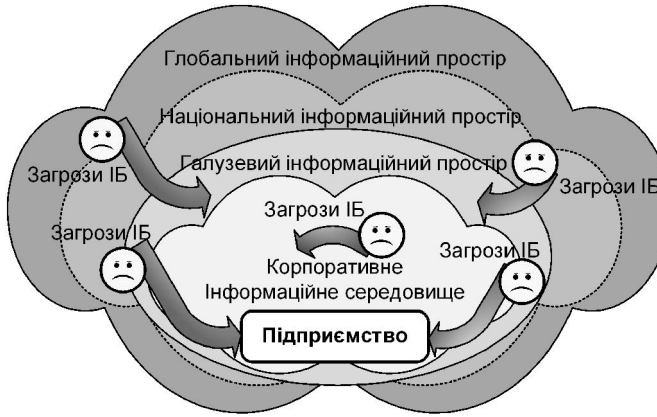


Рис. 1.1. Інформаційне середовище підприємства

Загроза ***(threat)*** – будь-які обставини або події, що можуть бути причиною порушення політики безпеки інформації і/або нанесення збитків.

Політика безпеки інформації *(Information security policy)* – сукупність законів, правил, обмежень, рекомендацій, інструкцій тощо, які регламентують порядок обробки інформації.

При цьому на діяльність підприємства усе більш суттєвий вплив здійснюють саме останні складові. Вони ж й є одночасно головними джерелами ***загроз*** їх інформаційної безпеки взагалі та для їх ***інформаційної інфраструктури*** зокрема.

Інформаційна інфраструктура *(Information infrastructure)* – складова інформаційного простору, яка являє собою сукупність даних (структурованих чи неструктурованих), засобів збору, накопичення, обробки, збереження та розповсюдження інформації, систем виробництва інформаційних продуктів, інформаційних ресурсів, інструктивних матеріалів та документації, а також людини як активного фактору вплину на інформаційний простір.

«Інформаційний вибух» наших часів, пов'язаний з широким використанням інформаційно-комунікаційних технологій (ІКТ), став каталізатором процесу інформаційних протистоянь. Не буде перебільшенням якщо сказати, що сьогодні вже йдуть численні інформаційні війни різних масштабів (інформаційна боротьба, інформаційне протиборство, інформаційні операції – це вже досить поширені поняття), які, завдяки віртуальній сфері їх проходження, ми не помічаємо, поки ми самі, або наші підприємства, установи раптом не опиняться у самому пеклі цих протистоянь.

Отже, інформаційна безпека є багатогранною, можна навіть сказати, багатомірною галуззю діяльності, у якій успіх може принести тільки систематичний, комплексний підхід. Адже висловлювання відомого мислителя та політичного діяча середньовіччя Ніколо Макіавеллі – «хто хоче жити у мирі, має готуватися до війни», – на жаль, залишається актуальним й досі.

Інформаційна безпека перш за все є складовою частиною національної безпеки, що характеризує стан захищеності національних інтересів в інформаційній сфері від зовнішніх та внутрішніх загроз.

До об'єктів інформаційної безпеки у загальнодержавному значенні відносяться:

- свідомість, психіка людей та їх колективів;
- суспільство та держава;
- різноманітні інформаційні системи (наприклад, засоби масової інформації), які складають інформаційну інфраструктуру держави.

До суб'єктів інформаційної безпеки відносяться:

- держава, що здійснює свої функції через відповідні органи державної влади шляхом створення системи забезпечення інформаційної безпеки;
- громадяни, суспільні або інші організації і об'єднання, що володіють повноваженнями із забезпечення інформаційної безпеки відповідно до законодавства.

Однак масова комп'ютеризація всіх сфер життя, поступове переведення основних інформаційних потоків у виробництві і управлінні в комп'ютерну форму, широке використання ІКТ обумовили якісні зміни тієї ролі, яку відіграє безпека і захист інформації. Адже кількість загроз інформації, що зберігається і обробляється в автоматизованих системах, суттєво зросла, з одночасним зростанням втрат від реалізації цих загроз.

Сучасне становище інформаційного впливу на діяльність підприємств, установ і організацій відкриває широкі можливості для впровадження в них ІКТ і, відповідно, створення в них АІС. Ці АІС стали формою вдосконалення існуючих на підприємстві систем управління, що знайшло значне

поширення та розвиток, з часом трансформувавшись в різні типи інформаційних автоматизованих систем, зокрема в ***системи підтримки прийняття рішень*** (СППР). Інтерес до СППР з боку користувачів як до перспективного інструментарію підвищення ефективності праці у сфері управління економікою, завдяки застосуванням в них математичних моделей, постійно зростає. Також набуває усе більшого поширення і тенденція «інтелектуалізації» АІС, в особливості систем підтримки прийняття рішень, пов'язана із реалізацією в них механізму «трансформації» інформації в знання і використання цього знання як ресурсу прийняття рішень, а також використання засобів штучного інтелекту. Наявність в СППР аналітичної інформації і нових знань, унікальних математичних методів не залишається поза уваги і злочинців усіляких різновидів.

Автоматизована інформаційна система; АІС *(automated information system)* – організаційно-технічна система, що реалізує інформаційну технологію і об'єднує обчислювальну систему, фізичне середовище, персонал і інформацію, що обробляється.

Виходячи з широкого використання у найрізноманітніших сферах життєдіяльності ІКТ та розуміння необхідності вирішення проблеми нейтралізації або мінімізації нової сукупності загроз виник термін «кібербезпека» *(cybersecurity)*. Вважаються, що спочатку він був застосований у США у середині 1990-х років, коли уряд цієї країни одним із перших став досліджувати цю тему.

Префікс cyber, що походить від терміну cybernetics, що став назвою нової науки «кібернетика», запропонованої у 1948 р. американським математиком Норбертом Вінером, започаткували використовувати для створення нових понять, пов'язаних зі сферою обчислювальної техніки та опрацювання інформації, що призвело зокрема до таких понять, як *cyberspace* – кібернетичний простір (кіберпростір), *cyberthreat* – кібернетична загроза (кіберзагроза), *cyberattack* – кібернетична атака (кібератака), *cybercrime* – кіберзлочинність, тощо. З того часу велика кількість країн прийняли стратегії кібербезпеки (США, Німеччина, Франція, Канада та багато інших), серед них і Україна. Метою Стратегії кібербезпеки України є створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави.

Зважаючи на те, що терміни, що походять від префіксу «кібер» все частіше і частіше використовується, необхідно визначитись, коли і як використовувати ці терміни поряд з термінами, що походять від слова «інформаційне» (інформаційна безпека та ін.).

Треба розуміти, що кібербезпека – це деякий стан автоматизованих інформаційних систем, за якого нейтралізуються загрози інформації, що циркулює в цих системах.

В цілому слід зазначити, що переважна більшість експертів пов'язують проблематику кібербезпеки саме з використанням у процесі людської діяльності комп'ютерних систем і телекомунікаційних мереж, у тому числі й Інтернету. На основі зіставлення визначення терміна «кібербезпека» та терміна «інформаційна безпека» можемо зробити висновок про те, що кібербезпека – це окремий випадок інформаційної безпеки, поява якого обумовлена використанням комп'ютерних систем та/або телекомунікаційних мереж. У цьому сенсі суть інформаційної безпеки полягає у захисті інформаційного простору країни від небажаного інформаційного впливу, захисті національних інформаційних ресурсів, а суть кібербезпеки – у забезпеченні безпечного функціонування автоматизованих інформаційних та телекомунікаційних систем, а також у захисті інформації, що циркулює в них.

За аналогією і всі інші «кібер-терміни» слід вважати елементами «інформаційних» понять, якщо мова йде про сферу використання комп'ютерів та телекомунікацій.

Кібербезпека – стан захищеності життєво важливих інтересів особистості, суспільства і держави в умовах використання комп'ютерних систем та/або телекомунікаційних мереж, за якого мінімізується завдання їм шкоди.

Так, розглядаючи загальне поняття «інформаційна інфраструктура» його окремим випадком буде інфраструктура кіберпростору, до переліку складових якої слід віднести лінії та засоби зв'язку, побудовані на їх основі мережі телекомунікацій, технічні і програмні засоби, електронні інформаційні ресурси, а також відповідні інституційні складові (обчислювальні центри, оператори та провайдери телекомунікацій, тощо).

Названі складові фактично є елементами сучасних автоматизованих інформаційних систем (АІС), з чого можна зробити висновок, що АІС є також елементами інфраструктури кіберпростору.

1.1.2. Визначення та загальні властивості інформації

Говорячи про інформаційну та кібербезпеку не можна оминути саме поняття ***інформації***. Власне поняття інформації настільки об'ємне і багатогранне, що загальноприйнятого визначення інформації не існує, і воно використовується головним чином на інтуїтивному рівні. Різні визначення висвітлюють лише його окремі грані – від побутового, як відомості або повідомлення про щось, до філософського, наданого академіком В.М. Глушковим, як міра неоднорідності розподілу матерії та енергії у просторі та у часі, міра змін, якими супроводжуються всі процеси, що протікають у світі.

Хоча існує значна кількість визначень поняття «інформація», але практично всі чисельні погляди на сутність інформації групуються навколо двох концепцій (парадигм) – *атрибутивної та функціональної*.

Згідно з атрибутивною концепцією, інформація – це об'єктивна внутрішня властивість всіх матеріальних об'єктів, вона міститься у всіх без винятку елементах та системах матеріального світу. Прихильники ж функціональної концепції не визнають існування інформації у неживій природі, а саму інформацію визначають як зміст сигналу або повідомлення, отриманого кібернетичною системою із зовнішнього світу. Вони стверджують, що інформація та *інформаційні процеси* присутні у всіх самокерованих (технічних, біологічних, соціальних) системах.

Інформаційні процеси *(Information processes)* – процеси створення, збирання, зберігання, обробки, відображення, передавання, розповсюдження і використання інформації.

Власне поява цієї концепції пов'язана з розвитком кібернетики – науки про управління та зв'язок у живих організмах, суспільстві і машинах (це дало другу назву концепції – функціонально-кібернетична).

Ця концепція, розвинута в роботах Норберта Вінера, припускає, що процес управління в згаданих системах є процесом переробки (перетворення) певним центральним пристроєм інформації, одержуваної від джерел первинної інформації і передачі її в ті ділянки системи, де вона сприймається її елементами як наказ для виконання тієї або іншої дії. При цьому важливо, що головну роль тут відіграє зміст переданої інформації. Інформація, за Вінером – це «позначення змісту, отриманого з зовнішнього світу в процесі нашого пристосування до нього і пристосування до нього наших почуттів».

Підсумовуючи, основні аспекти інформації можна звести до табл. 1.1.

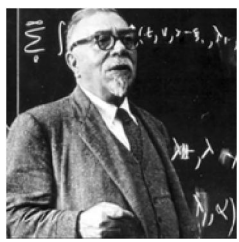
Таблиця 1.1

Основні аспекти інформації

Аспекти інформації	
Філософські	Інформація як одна з реальностей оточуючого світу. Питання походження та сутності інформації. Інформація як міра сутностей об'єктивного світу. Інформація і пізнання.
Управлінські	Інформація як неодмінний атрибут будь-якого управління. Інформаційні процеси як основний зміст управління та прийняття рішень.
Технічні	Інформація як сукупність символів, зафіксованих на носіях. Проблеми збирання, зберігання, представлення, передачі та обробки інформації.
Соціальні	Інформація як важливий атрибут життєдіяльності суспільства. Проблеми визначення інформаційних потреб в суспільстві. Проблеми раціоналізації інформаційних процесів. Проблеми інформаційного забезпечення діяльності суспільства.

Так що ж таке інформація? Вочевидь, з того, чого ми дізнались, передусім витікає, що інформація з'являється як деяке *повідомлення*, яке передається від джерела (передатчика) до споживача (приймача). Іншими словами, інформація – це сукупність *сигналів*, які сприймаються споживачем та відображають деякі властивості явищ чи об'єктів. При цьому це повідомлення має зменшити міру невизначеності споживача про деяке явище чи об'єкт.

Розуміється, що для забезпечення виникнення та існування інформації мають бути можливості щодо її *передачі, зберігання* та *обробки*.



Норберт Вінер
(Norbert Wiener),
американський математик та філософ, «батько кібернетики»

В.М. Глушков,
видатний український вчений,
автор багатьох наукових досягнень в галузі математики та кібернетики

Основою математичних досліджень процесів зберігання, перетворення і передачі інформації є теорія інформації. Теорія інформації тісно пов'язана з такими розділами математики як теорія ймовірностей і математична статистика. Виникнення теорії інформації зазвичай пов'язують із появою у 1948 році фундаментальної праці Клода Шеннона «Математична теорія зв'язку».

Теорія Шеннона з самого початку розглядалась як точно сформульована математична задача і дала можливість інженерам визначати ємність комунікаційного каналу. В основі теорії інформації лежить запропонований Шенноном метод обчислення кількості інформації у випадковій величині відносно іншої випадкової величини (так звана формула ентропії). Він же запропонував використати слово «біт» для позначення найменшої одиниці інформації.

Уводячи поняття інформації як міри невизначеності, рівній величині ***ентропії***, Вінер і Шеннон створили математичний апарат виміру об'єму і розрахунку втрат інформації в каналах передачі даних.

Ентропія – у природничих науках міра безладу системи, що складається з багатьох елементів.

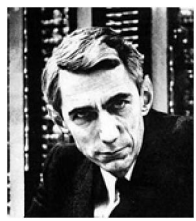
Інформаційна ентропія – міра невизначеності джерела повідомлень, визначувана імовірністю появи тих або інших символів при їх передачі.

Одначе цей підхід не враховує такі поняття, як цінність або повнота інформації, які, взагалі кажучи, не мають відношення до кібернетики, але є дуже важливими для сучасних систем обробки інформації. Добре розумів обмеженість кібернетичного підходу до інформації французький фізик Леон Бріллюен. При обговоренні формули ентропії у своїй книзі «Наука і теорія інформації» він неодноразово вказував, що «це дуже точне визначення обмежує нас». Бріллюен наводить приклад, що «сукупність 100 букв, вибраних випадковим чином, фраза зі 100 букв з газети, п'єси Шекспіра або теореми Ейнштейна мають в точності однакову кількість інформації». Але таке визначення інформації є таким, як щось відмінне від *знання*. Одначе саме знання є найважливішим для людини, для якої і створюються інформаційні системи. Проте для знання у нас немає кількісної міри.

Отже – і до цього схиляються чимало вчених – насправді ніяка наука не зможе описати процеси створення інформації, якщо з неї буде виключена людина. А інформаційна система – це система комунікацій між людьми, яка дозволяє їм творити і ділитися результатами своєї діяльності один

з одним, тобто породжуваною ними інформацією. Так що можна зробити висновок, що інформація народжується тільки там, де є люди і комунікації.

Таким чином, поняття інформації є багатогранним, а питання інформаційної безпеки та захисту інформації тісно пов'язані з різноманіттям її основних аспектів. Виходячи з цього постулату спектр інтересів суб'єктів, пов'язаних з використанням інформаційної системи, традиційно поділяється у відповідності до трьох категорій, або основних властивостей інформації у сенсі інформаційної безпеки, а саме забезпечення ***доступності, цілісності*** й ***конфіденційності*** інформаційних ресурсів і підтримуючої інфраструктури.



Клод Элвуд Шеннон
(Claude Elwood Shannon),
американський вчений,
«батько теорії інформації»

Леон Ніколя Бріллюен
(Léon Nicolas Brillouin),
французький та американський
фізик та філософ

Доступність *(availability)* – властивість інформації, пов'язана з можливістю бути отриманою авторизованим користувачем за наявності у нього відповідних повноважень, в необхідний для нього час.

Цілісність *(integrity)* – означає неможливість модифікації інформації неавторизованим користувачем.

Конфіденційність *(confidentiality)* – властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем.

Для АІС, що створюються для надання користувачам певних інформаційних послуг, у тому числі й СППР, доступність, вочевидь, виділяється як найважливіший елемент кібербезбеки. Особливо важлива роль доступності проявляється в різного роду СППР у сфері оперативного управління – виробництвом, транспортом і т.ін., а також у системах, які надають інформаційні послуги великій кількості людей (продаж залізничних і авіаквитків, банківські послуги й т.ін.).

Цілісність можна поділити на статичну (що розуміється як незмінність інформаційних об'єктів) і динамічну (стосовно коректного виконання складних дій (транзакцій)). Засоби контролю динамічної цілісності застосовуються, наприклад, при аналізі потоку фінансових повідомлень з метою виявлення крадіжки, переупорядкування або дублювання окремих повідомлень.

Нарешті, питання конфіденційні важливі також для багатьох організацій і АІС, зокрема у фінансово-економічній сфері, а також і для окремих користувачів (наприклад, паролі).

1.1.3. Кіберзлочинність, кібербезпека та захист інформації

Наскільки ж кіберзлочинність сьогодні небезпечна? Вважається, що вона являє загрозу не тільки для окремої людини, підприємства чи організації, або країни, але й для всього людства. Ступінь цієї загрози у силу своєї новизни ще не до кінця вивчена. Захиститися від кібертерору не може жодна держава, а кіберзлочинець здатний загрожувати інформаційним системам, розташованим практично в будь-якій точці земної кулі.

Існує думка, що, наприклад, кібертероризм страшніше, ніж атомна бомба, бактеріологічна або хімічна зброя.

Винайдення потужних комп'ютерів і вбудованих мікроконтролерів, що сприяло розвитку систем управління у промисловості привело переважну більшість країн світу не тільки до глобальної інформатизації, але й зробило більш вразливими передусім критично-важливі сегменти та об'єкти їх економіки до кіберзагроз. Нажаль, вирішення цих задач в повному обсязі на сучасному етапі розвитку суспільства не завжди вбачається можливим.

Загроза безпеці інформації – потенційна можливість порушення основних якісних характеристик (властивостей) інформації при її обробці програмно-технічними засобами, а саме конфіденційності, доступності та цілісності

Саме цей факт призводить до здійснення низки злочинів і терактів в кіберпросторах з використанням можливостей сучасних ІКТ. Прикладів таких подій вже безліч, деякі з них наведені у табл. 1.2.

Відповідно до загроз, зокрема, з огляду на застосування ІКТ, кібербезпеку можливо класифікувати за її видами у такій спосіб:

- протидія комп'ютерній злочинності та комп'ютерному тероризму;
- забезпечення безпеки надання доступу користувачів до інформації, що обробляється в АІС, у тому числі тих, доступ до яких здійснюється з використанням Інтернету;
- забезпечення безпеки автоматизованих (інформаційно-телекомунікаційних) систем загального призначення;
- забезпечення безпеки автоматизованих систем органів державної влади та місцевого самоврядування, систем, які функціонують в інтересах управління державою, забезпечують потреби оборони та безпеки держави, кредитно-банківських та інших сфер економіки держави, систем управління життєзабезпеченням.

Таблиця 1.2

Приклади злочинів і терактів в кіберпросторах з використанням можливостей сучасних ІКТ

Дати	Засіб здійснення злочину	Наслідки злочину
серпень 2003	Вірус Blaster, також відомий як Lovsan, Lovesan, MSBlaster	Викликав відключення світла у Нью-Йорку
червень 1982	Кібератака проти сибірського газопроводу шляхом активації програмного забезпечення, до якого американці попередньо ввели помилкові дані	Програма перевищила режим роботи газопроводу настільки, що він вибухнув
2003-2007	Атаки китайського хакерського угруповання «Хунке» на сервера американської компанії LockheedMartin	Викрадення проектів програм для розробки винищувача-бомбардувальника п'ятого покоління *F-35 Lightning II*
2008-2010	Атака GhostNet за допомогою повідомлення електронної пошти, при відкритті якого запускалася шкідлива програма	Спрямована на посольства та міністерства у 103 країнах світу для дистанційного управління їх системами
липень 2010	Вірус Stuxnet, що був уведений через USB у контролери атомних станцій Ірану	Зупинив їх функціонування, блокував ядерну програму Ірану
травень 2012	Троянська вірусна програма «Flame»	Цілеспрямований систематичний збір даних в країнах Близького Сходу (офісні документи, креслення тощо), можливість модифікації інформації
2014-2015	Масові DDoS-атаки із застосуванням ботмереж на ресурси 76 країн світу	На відбиття атаки жертви витрачали в середньому 32 доби

Комплекс заходів, спрямованих на забезпечення кібербезпеки, визначається як захист інформації.

Отже, під кібербезпекою будемо розуміти захищеність інформації й інформаційної інфраструктури АІС від випадкових або навмисних впливів природного або штучного характеру, які можуть завдати неприйнятної

шкоди суб'єктам інформаційних відносин, у тому числі власникам і користувачам інформації й інформаційної інфраструктури АІС.

Захист інформації *(information security, data protection)* – Сукупність методів і засобів, що забезпечують цілісність, конфіденційність і доступність інформації за умов впливу на неї загроз природного або штучного характеру, реалізація яких може призвести до завдання шкоди власникам і користувачам інформації.

Захист інформації в АІС *(information protection, computer system security)* – діяльність, яка спрямована на забезпечення безпеки оброблюваної в АІС інформації та АІС в цілому, і яка дозволяє запобігти або ускладнити можливість реалізації загроз, а також знизити величину потенційних збитків внаслідок реалізації загроз.

Такий підхід до проблем кібербезпеки, з методологічної точки зору, починається з виявлення суб'єктів інформаційних відносин і інтересів цих суб'єктів, пов'язаних з використанням АІС, а також *об'єктів* АІС, на які спрямовані загрози кібербезпеки. На рис. 1.2 наведено суб'єкти і об'єкти інформаційних відношень у випадку розгляду проблеми кібербезпеки СППР.

Рис. 1.2. Суб'єкти і об'єкти інформаційних відношень у випадку розгляду проблеми кібербезпеки СППР

Зміст проблем, пов'язаних з кібербезпекою, для різних типів підприємств та систем може істотно розрізнятися. Значною мірою це стосується СППР, адже на цей час сформувалося чимало типів СППР, що

відрізняються за різними ознаками – за кількістю користувачів, за технічними характеристиками, в залежності від типів даних, з якими ці системи працюють та ін. Крім того, ці системи можуть використовуватись у великому різноманіття підприємств та організацій.

Тому для СППР у режимних державних організаціях або у таких комерційних структурах, як, наприклад, банки, актуальним є забезпечення у будь якому разі конфіденційності інформації, що обробляється. А, наприклад, в навчальних закладах, вважається достатнім забезпечити лише обмежений доступ до деяких ресурсів різним категоріям користувачів (приміром, студентам та викладачам).

Але у будь якому разі треба мати відповіді на три основні питання: 1) що має захищатись, 2) від кого захищати та 3) як і чим захищати. Тому дивитись на проблему треба ширше, ніж зведення кібербезпеки виняткова до захисту від несанкціонованого доступу (НСД) до інформації. Суб'єкт інформаційних відносин (наприклад, особа, що приймає рішення) може постраждати (зазнати збитків, неможливість одержати рішення) не тільки від НСД, але й, наприклад, від виходу з ладу елементу СППР, що викликало перерву в роботі. Більш того, для багатьох СППР (наприклад, таких, які накопичують бази даних і знань та обслуговують кількох ОПР) по важливості на першому місці стоїть безперебійність роботи та схоронність інформації (доступність та цілісність), а не власне захист від НСД до інформації.

Виходячи з цього, слід зазначити, що часто використовуваний термін «захист комп'ютерної інформації» у сучасних умовах представляється занадто вузьким. Комп'ютери – тільки одна зі складових інфраструктури будь якої АІС, у тому числі й СППР, і безпека інформації визначається всією сукупністю складових інформаційної інфраструктури та, у першу чергу, її найслабкішими ланками, якими в переважній більшості випадків виявляється сама людина, а також, наприклад, чинники зберігання носіїв інформації або забезпечення охорони офісного приміщення.

1.1.4. Державна політика забезпечення інформаційної та кібербезпеки

Інформаційна та кібернетична безпека є одними з найважливіших аспектів інтегральної безпеки, на якому б рівні не розглядалася остання – національному, галузевому, корпоративному або персональному. Тому важливу роль у цій сфері відіграє державна політика, яка спрямована на розробку та впровадження сучасних безпечних інформаційних технологій,

побудову захищеної національної інформаційної інфраструктури, формування і розвиток інформаційних стосунків тощо. Вона реалізується шляхом:

1) створення і забезпечення ефективного функціонування в Україні цілісної системи інформаційної та кібернетичної безпеки;

2) вдосконалення існуючої і розробки нової нормативно-правової бази, яка регулює відносини в сфері безпеки, встановлює вимоги і правила провадження діяльності у цій сфері;

3) забезпечення боротьби з кіберзлочинністю.

Стратегією національної безпеки України, затвердженою указом Президента України №287/2015 серед основних напрямів державної політики національної безпеки України визначаються забезпечення інформаційної безпеки та забезпечення кібербезпеки і безпеки інформаційних ресурсів. Заходами забезпечення інформаційної безпеки передбачається протидія інформаційним операціям проти України, маніпуляціям суспільною свідомістю і поширенню спотвореної інформації, всім формам і проявам інформаційної агресії. Серед основних пріоритетів забезпечення кібербезпеки і безпеки інформаційних ресурсів передбачається зокрема створення системи забезпечення кібербезпеки, моніторинг кіберпростору з метою своєчасного виявлення, запобігання кіберзагрозам і їх нейтралізації, а також забезпечення захищеності об'єктів критичної інфраструктури та державних інформаційних ресурсів від кібератак.

У свою чергу Стратегію кібербезпеки України, затвердженою указом Президента України №96/2016, уводиться поняття Національної системи кібербезпека, а серед пріоритетів та напрямів забезпечення кібербезпеки України вбачається розвиток безпечного, стабільного і надійного кіберпростору, кіберзахист державних електронних інформаційних ресурсів та інформаційної інфраструктури, кіберзахист критичної інфраструктури, боротьба з кіберзлочинністю тощо. Згідно зі Стратегією, розвиток та безпека кіберпростору, запровадження електронного урядування, гарантування безпеки й сталого функціонування електронних комунікацій та державних електронних інформаційних ресурсів мають бути складовими державної політики у сфері розвитку інформаційного простору та становлення інформаційного суспільства в Україні.

Загалом, в Україні створена й функціонує структурно повна система забезпечення інформаційної безпеки. Функції та повноваження відповідних державних органів закріплені в нормативно-правових актах різного рівня – Конституції України, законах України, указах Президента України, постановах Кабінету Міністрів України, інших, у т.ч. відомчих, норматив-

них актах. Водночас розподіл функцій між окремими суб'єктами системи та схема їх взаємодії потребують вдосконалення.

Важлива роль у забезпеченні безпеки відводиться удосконаленню законодавчого (нормативного) регулювання суспільних інформаційних відносин та питань забезпечення безпеки на національному рівні. При цьому вони повинні відповідати вимогам щодо гармонізації українського законодавства з міжнародним законодавством і законодавством ЄС, вони мають створити для України можливість стати рівноправним учасником міжнародного інформаційного обміну за умов збереження інформаційного суверенітету нашої країни.

Аналіз розвитку комп'ютерної злочинності дозволяє зробити висновок, що ця проблематика, особливо її складова – організована комп'ютерна злочинність сьогодні вже має чітко визначений, як національний, так і міжнародний, транснаціональний характер. На погляд закордонних фахівців, протиправне використання комп'ютерів дає більші прибутки для злочинців з меншими ризиками, ніж скоєння традиційних злочинів шляхом викрадення грошей в банках, тому число таких злочинів з кожним роком буде зростати. Введення мережі електронних розрахунків веде до трансформації техніки виконання корисливих злочинів у сфері банківської та пов'язаної з нею кредитною, фінансово-економічною діяльністю, хоча в її основі є ті ж механізми документообігу, що базуються на системі звичайного бухгалтерського обліку. Тому діюча технологія вчинення злочинів автоматично переноситься в умови електронних розрахунків.

Складність ситуації в сфері боротьби з комп'ютерною злочинністю є такою, що потрібен пошук принципово нових підходів для розробки відносно надійних систем захисту. Наприклад, в багатьох країнах приймаються урядові рішення щодо сприяння поширенню та застосування в державних системах відкритого та такого, що вільно розповсюджується, програмного забезпечення, адже, за статистикою, воно значно менш уразливе щодо заражень вірусами та інших проникнень, ніж комерційне (пропрієтарне) ПЗ.

Крім того, зусилля в багатьох країнах концентруються й на такому важливому питанні, як подолання необізнаності широкого кола громадськості щодо загроз інформаційній безпеці здобутків в її забезпеченні.

Основними суб'єктами державної політики інформаційної та кібербезпека, на які покладаються в установленому порядку завдання забезпечення безпеки є Рада національної безпеки і оборони України, яка відповідно до Конституції України та у встановленому законом порядку має здійснювати координацію та контроль діяльності суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку України. Крім того, основу націо-

нальної системи кібербезпеки становитимуть Міністерство оборони України, Державна служба спеціального зв'язку та захисту інформації України, Служба безпеки України, Національна поліція України, Національний банк України, розвідувальні органи.

Також в Україні діє Національний координаційний центр кібербезпеки, який є робочим органом Ради національної безпеки і оборони України. Центр здійснює прогнозування і виявлення потенційних і реальних загроз у сфері кібербезпеки України, узагальнює міжнародний досвід у сфері забезпечення кібербезпеки; оперативне інформаційно-аналітичне забезпечення РНБО з питань кібербезпеки.

1.1.5. Коротка історична довідка

Перші спроби захисту інформації були пов'язані з шифруванням. Ніхто не може сказати точно, коли ж був придуманий найперший шифр на світі. Мабуть, відразу після появи писемності. Але швидше за все, з появою державної і військової переписки. Сьогодні вже будь-яка людина може закодувати дані, які він завантажує в Інтернет, пересилає по електронній пошті або вводить в онлайн-форми при проведенні банківських операцій. При цьому принципи, на яких базується сучасне шифрування, старі як світ. Різниця тільки в тому, що в давні часи кодувалися літери, а сьогодні – блоки бітів.

Розвиток технологій шифрування супроводжувався появою та постійним вдосконаленням технічних засобів, що використовувались для реалізації шифрів та для їх розкриття. У наші часи на цю службу прийшли електронні обчислювальні машини та перспективні квантові комп'ютери.

З появою комп'ютера, створенням баз даних, а потім й автоматизованих систем стрімкого розвитку набуло розв'язання проблем захисту інформації в АІС. Поступово, з ускладненням систем та появою телекомунікаційного обміну інформацією, змінювались і погляди на можливості захисту інформації в автоматизованих системах – від взагалі постановки задачі захисту до отримання важливих результатів, як то про неможливість абсолютного захисту систем, а також про важливість комплексного підходу до побудови систем захисту. Таким чином цей розвиток пройшов певні етапи, характеристику яких наведено у табл. 1.3.

У зв'язку зі створенням і впровадженням АІС у процеси інформаційного забезпечення та управління діяльності великих і середніх підприємств і організацій в 70-х роках XX ст. виникли практичні задачі забезпечення безпеки комп'ютерної інформації. Потрібна була теоретична база, програмно-технічні рішення й механізми забезпечення безпеки при колективній обробці загальних інформаційних ресурсів.

Таблиця 1.3.

Етапи розвитку захисту інформації в автоматизованих системах

Етап	Термін дії	Основні досягнення
Перший (емпіричний)	Кінець 60-х рр. XX ст.	Постановка проблеми захисту інформації в автоматизованих системах. Ідея надійного захисту програмними та технічними засобами
Другий (концептуально-емпіричний)	Кінець 70-х рр. XX ст.	Проблеми захисту розподілених систем. Теоретичний результат про неможливість абсолютного захисту
Третій (теоретико-концептуальний)	Кінець 80-х рр. XX ст.	Центральна ідея – створення «систем захисту». Математичні моделі захисту
Четвертий (комплексний)	Наш час	Багатоаспектність захисту. Комплексність та динамічність систем захисту

Саме в той час з'явилися перші роботи з політики (методології) і моделей захисту комп'ютерної інформації. Значний внесок у створення теорії безпеки комп'ютерної інформації внесли такі дослідники, як Л.Дж. Хоффман, Р. Хартсон, М. Харрисон, У. Руззо, Дж. Ульман, Д. Белл, Л. ЛаПадула й ін. Це привело зокрема й до появи нових шифрів та криптосистем, революційний внесок до яких забезпечили Уітфілд Діффі, Мартін Хеллман, Тахір Ельгамаль, Рон Рівест, Аді Шамір, Леонард Адлман та ін.

Створені в той період моделі розмежування доступу послужили методологічною основою для розробки перших стандартів безпеки комп'ютерних систем, зокрема, відомої «Оранжевої книги», уперше опублікованої у 1983 році. Свій внесок у розвиток моделей розмежування доступу цього періоду внесли Дж. МакЛин, К. Лендвер, Дж. Гоген, Дж. Мезигер, В. Варахараджан й ін.

У 90-і роки до досліджень процесів захисту комп'ютерної інформації більш активно підключилися радянські дослідники. Серед них слід відмітити, насамперед, праці В.А. Герасименко, який розробив системно-концептуальний підхід до забезпечення інформаційної безпеки автоматизованих систем обробки даних. А.А. Грушо і Е.Е. Тімоніна представили доказовий підхід до проблеми гарантованості захисту інформації в комп'ютерній системі, а також провели математичний аналіз ряду задач і розв'язань у теорії захисту інформації стосовно до різних різновидів комп'ютерних систем.

В Україні з перших днів існування української держави проблемам забезпечення безпеки інформації, захисту інформаційного простору від небажаного інформаційного впливу, забезпеченню безпечного функціонування інформаційно-телекомунікаційних систем та захисту інформації, що циркулює в них, приділялась серйозна увага. Вже наступного дня після проголошення Декларації про незалежність України було прийнято рішення щодо прийняття під юрисдикцію України захищених видів зв'язку.

З метою концентрації державних зусиль у сфері криптографічного та технічного захисту інформації за рішенням Президента України у серпні 1998 року було створено Департамент спеціальних телекомунікаційних систем та захисту інформації СБ України, який 2005 року було реорганізовано в Державну службу спеціального зв'язку та захисту інформації України (ДССЗЗІ України).

Контрольні запитання та завдання

1. Загальні поняття інформаційної безпеки, кібербезпеки та захисту інформації.
2. Поняття загрози.
3. Основні концепції (парадигми) визначення поняття «інформація".
4. Які можливості мають бути реалізованими для виникнення та існування інформації?
5. У чому основна суть початків теорії інформації, сформульованих К. Шенноном?
6. У чому полягають погляди Л. Бріллюена на міру інформації?
7. Що відноситься до суб'єктів і об'єктів інформаційних відношень у випадку розгляду проблеми кібербезпеки СППР?
8. Які етапи пройшов розвиток захисту інформації в АІС?
9. Мета та основні принципи державної політики забезпечення інформаційної безпеки.

1.2. ЗАГРОЗИ ПОРУШЕНЬ КІБЕРБЕЗПЕКИ

Основні визначення й критерії класифікації загроз. Найпоширеніші загрози. Шкідливе програмне забезпечення

1.2.1. Основні визначення й критерії класифікації загроз

Знання можливих загроз як потенційної можливості певним чином порушити кібербезпеку СППР, а також уразливих місць захисту, які ці загрози зазвичай використовують, необхідне для того, щоб вибирати найбільш економічні та ефективні засоби забезпечення безпеки.

Спроба реалізації загрози називається *атакою*, а той, хто вживає таку спробу, – *зловмисником*, або *порушником*. Потенційні зловмисники іменуються *джерелами загрози*. Загроза реалізується через атаку в певному місці й у певний час, тобто вона характеризується способом нападу в певному місці й у певний момент.

Таким чином, зв'язок поміж видом небезпеки й можливою загрозою складається з *місця, часу* й *типу* атаки, що реалізує загрозу. Аналіз небезпеки повинен показати, де й коли зберігається або з'являється цінна інформація, у якому місці системи ця інформація може втратити цінність.

Найчастіше загроза і наступна компрометація системи є наслідком наявності *уразливостей* у захисті СППР (таких, наприклад, як можливість доступу сторонніх осіб до критично важливої інформації або обладнання, помилки в програмному забезпеченні). Окремим випадком уразливості системи є *вади захисту*, під якими розуміють особливості побудови програмних або апаратних засобів захисту, що за певних обставин спричиняють їхню нездатність протистояти загрозам. Класифікацію вад захисту програмного забезпечення за місцем в СППР наведено на рис. 1.3.

Рис. 1.3. Класифікація вад захисту програмного забезпечення за місцем в СППР

Проміжок часу від моменту, коли з'являється можливість використати слабке місце, і до моменту, коли прогалина ліквідується, має назву ***вікно небезпеки***, асоційоване з даним уразливим місцем. Поки існує вікно небезпеки, можливі успішні атаки на СППР.

Уразливість системи *(system vulnerability)* – нездатність системи протистояти реалізації певної загрози або ж сукупності загроз.

Вади захисту *(security flaw)* – сукупність причин, умов і обставин, наявність яких може привести до порушення нормального функціонування системи або політики безпеки інформації.

Вікно небезпеки ліквідується при вживанні заходів, що виправляють уразливість (накладання латок). Для більшості уразливих місць вікно небезпеки існує порівняно довго (кілька днів, іноді – тижнів, а то навіть і роки). Це пояснюється тим, що за цей час має стати відомо про засоби використання прогалини в захисті, повинні бути випущені відповідні латки, нарешті, латки повинні бути встановлені в систему (рис. 1.4).

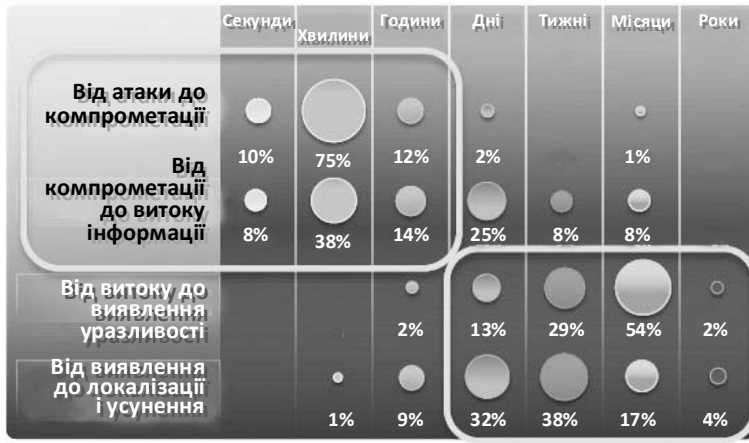


Рис. 1.4. Часова шкала інтервалів від атак до усунення уразливостей (у % від загального числа зломів)

Нові уразливі місця й засоби їхнього використання з'являються на всіх етапах створення систем, зокрема їх програмного забезпечення, на що є кілька головних причин (рис. 1.5). Таким чином, вікна небезпеки існують майже завжди, тому відстеження таких вікон повинне провадитися постійно, а випуск і накладення латок – якомога більш оперативно.

Слід зазначити, що деякі загрози не можна вважати наслідком якихось помилок або прорахунків; вони існують завдяки самій природі сучасних СППР. Наприклад, суттєвим є недостатня кваліфікація користувача системи – особи, що приймає рішення. Також часто існує загроза про-

никнення у приміщення офісу сторонньої особи. Причиною може бути й суттєве відставання нормативної бази на підприємстві, що врегульовує питання безпеки.

Рис. 1.5. Внесення уразливостей за етапами створення програмного забезпечення СППР

Для аналізу загроз важливе значення має побудова *моделі загроз* як абстрактного структурованого опису загрози. Модель загроз визначає склад і джерела загроз, оцінку можливості їх прояву, шляхи їх здійснення, оцінку очікуваного збитку від реалізації загроз. У нормативному документі НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі» рекомендоване таку структуру опису:

- властивість інформації, на яку спрямовано загрозу;
- джерела виникнення загрози;
- способи реалізації загрози.

Також слід мати й *модель порушника* як всебічну структуровану характеристику порушника. Нормативними документами рекомендовано таку структуру моделі порушника:

- категорія порушника;
- мета порушника;
- повноваження порушника в АС;
- технічна оснащеність порушника;
- кваліфікація порушника.

Саме поняття «загроза» у різних ситуаціях найчастіше трактується по-різному. Наприклад, для відкритої організації загроз конфіденційності може просто не існувати – вся інформація вважається загальнодоступною; однак, у більшості випадків, несанкціонований доступ представляється серйозною небезпекою. Іншими словами, визначення загрози залежить від інтересів суб'єктів інформаційних відносин і від того, який збиток є для них неприйнятним.

Внаслідок цього набуває важливості питання класифікації загроз. Взагалі загрози можна класифікувати за кількома критеріями:

- по аспекту безпеки інформації (доступність, цілісність, конфіденційність), проти якого загрози спрямовані в першу чергу;
- по компонентах СППР, на які загрози націлені (дані, знання, програми, моделі, апаратура, підтримуюча інфраструктура);
- по способу здійснення (випадкові/навмисні дії, природного/техногенного характеру);
- по розташуванню джерела загроз (усередині/поза системи).

У загальному випадку загрози слід поділяти на природні та штучні загрози. Останні у свою чергу поділяються на ненавмисні загрози й на навмисні. Більш детальну класифікацію показано на рис. 1.6. Існують й інші точки зору на класифікацію загроз. Одну з них показано на рис. 1.7.

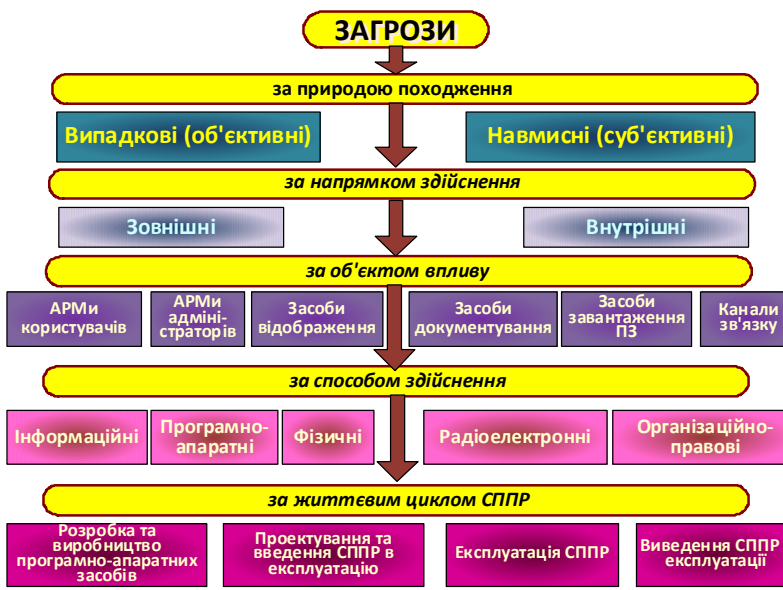


Рис. 1.6. Класифікація загроз СППР

Рис. 1.7. Альтернативна класифікація загроз СППР

Усі потенційно можливі негативні явища вказаного характеру можуть бути поділені на такі різновиди:

- зниження нижче допустимого рівня якості інформації, що використовується для вирішення завдань, які мають істотне значення;
- несанкціоноване отримання в зловмисних цілях такої інформації, на доступ до якої з тих або інших причин накладені обмеження;
- несанкціоноване використання інформації, яка є чиєю-небудь власністю;
- шкідлива дія інформації на людей, технічні пристрої (системи) і технологічні процеси.

Класифікація загроз може бути ще більш деталізованою. Для прикладу розглянемо класифікацію навмисних та ненавмисних загроз. Отже, до ненавмисних загроз відносяться:

- ненавмисні дії, що призводять до відмови системи;
- неправомірне відключення обладнання чи зміна режимів роботи пристроїв і програм;
- нелегальне впровадження і використання неврахованих програм;
- ненавмисне псування носіїв інформації;
- ненавмисне зараження вірусом;
- розголошення, втрата атрибутів розмежування доступу;

- запуск технологічних програм, здатних за некомпетентного використання викликати втрату працездатності системи чи незворотні зміни в ній;
- необережні дії, що призводять до розголошення конфіденційної інформації;
- проектування архітектури системи з можливостями, що становлять небезпеку для самої системи;
- ігнорування організаційних обмежень;
- входження у систему в обхід засобів захисту;
- некомпетентне використання, настроювання і неправомірне відключення засобів захисту;
- пересилання даних за адресою абонента, яка є хибною;
- введення помилкових даних;
- ненавмисне ушкодження каналів зв'язку.

До навмисних загроз відноситься:

- фізичне руйнування системи;
- вимкнення чи виведення з ладу підсистем забезпечення функціонування;
- дії з дезорганізації функціонування системи;
- вторгнення агентів у оточення персоналу системи;
- вербування персоналу чи окремих користувачів, що мають визначені повноваження;
- застосування пристроїв, що підслуховують, дистанційних фото- та відеозйомок;
- перехоплення побічних електромагнітних, акустичних та інших випромінювань і наведень від пристроїв і каналів зв'язку;
- перехоплення даних, переданих по каналах зв'язку;
- розкрадання носіїв інформації;
- несанкціоноване копіювання носіїв Інформації;
- розкрадання і вивчення виробничих відходів;
- зчитування залишкової інформації з оперативної нам'яті та зовнішніх запам'ятовуючих пристроїв;
- незаконне заволодіння паролями;
- несанкціоноване використання терміналів користувачів;
- розкриття шифрів захищеної інформації;
- впровадження програмно-апаратних закладок і вірусів;
- незаконне підключення до ліній зв'язку а метою роботи «між рядків»;
- незаконне підключення до ліній зв'язку з метою прямої підміни законного користувача шляхом його повного відключення.

Крім загальних підходів до класифікації загроз існують спеціальні класифікації, що пропонуються відомими розробниками програмних засобів та засобів захисту. Так корпорацією Майкрософт розроблена та обґрунтована методика класифікації загроз STRIDE (назву методики утворено з перших літер назв категорій загроз). Це варіант класифікації загроз за їхніми наслідками. Методику використовують для побудови моделі загроз під час розроблення ПЗ. Її складовими є наступні категорії:

1) підміна об'єктів *(spoofing identity)*. Крім загроз, які виникають через недоліки мережних протоколів, до цього класу належить також загроза, викликана підміною особи користувача. Її здійснюють, скориставшись слабкістю системи автентифікації або здобувши автентифікаційні дані шляхом крадіжки чи шахрайства;

2) модифікація даних *(tampering with data)*. До нього класу належать загрози впливів (атак), мета яких – навмисне псування даних. Атаки можуть бути спрямовані на інформаційні об'єкти, що перебувають у стані зберігання (файли, бази даних), і такі, що передаються мережею;

3) відмова від авторства *(repudiation of origin)*. Загрози нього класу дають змогу порушнику відмовитися від здійснених ним дій (або бездіяльності). Причиною існування такої загрози є відсутність або слабкість механізмів реєстрації подій і слабкі механізми автентифікації;

4) розголошення інформації *(information disclosure)*;

5) відмова в обслуговуванні *(denial of service)*. Атаки, що спричиняють відмову в обслуговуванні, порівняно легко здійснити в розподілених системах і дуже важко їм протидіяти. Особливо небезпечними є атаки *розподіленої відмови в обслуговуванні (dis-tributed denial of service)*), які здійснюють на один об'єкт одразу з кількох вузлів Мережі;

6) підвищення привілеїв *(elevation of privilege)*. Порушник має можливість підвищити рівень привілеїв і тим самим отримати доступ до визначених ресурсів (наприклад, адміністративних).

Різноманіття потенційних загроз інформації в СППР може бути настільки значним, що це не дозволяє передбачити та запобігти кожної з них, тому, проводячи аналіз загроз, треба вибирати їх з позицій здорового глузду, виявляючи не лише власне загрози, а й імовірності їх реалізації, масштаби наслідків, а також джерела походження.

1.2.2. Найпоширеніші загрози кібербезбеки СППР

Які ж загрози, що впливають на сучасні СППР, є найпоширенішими? Це питання є дуже важливим, адже мати уявлення про можливі загрози, а також про уразливі місця, які ці загрози зазвичай використовують, необхідно для того, щоб вибирати найбільш економічні та ефективні засоби забезпечення безпеки.

Поширеність загроз кібербезпека доцільно аналізувати за напрямами впливу на основні властивості інформації, що обробляється в системі – доступність, цілісність та конфіденційність.

Найпоширеніші загрози доступності. Найчастішими й найнебезпечнішими (враховуючи розмір збитку) загрозами доступності інформації є ненавмисні помилки персоналу – штатних користувачів, операторів, системних адміністраторів й інших осіб, що обслуговують СППР. Такі помилки можуть бути власне загрозами (неправильно уведені дані або помилка в програмі, що викликала крах системи), а іноді вони створюють уразливі місця, якими можуть скористатися зловмисники (такими є зазвичай помилки адміністрування).

Очевидно, що найрадикальніший спосіб боротьби з ненавмисними помилками – це максимальна автоматизація й суворий контроль.

Класифікуємо загрози доступності по компонентах СППР, на які націлені загрози, а саме:

- відмова користувачів працювати з системою;
- внутрішня відмова системи;
- відмова підтримуючої інфраструктури.

Зазвичай стосовно до користувачів розглядаються наступні загрози:

- небажання працювати з СППР (найчастіше проявляється при необхідності освоювати нові можливості системи, при розбіжностях між запитами користувачів і фактичними можливостями системи);
- неможливість працювати з СППР з-за відсутності відповідної підготовки (нестача загальної комп'ютерної грамотності, невміння інтерпретувати повідомлення системи, невміння працювати з документацією й т.ін.);
- неможливість працювати з системою з-за відсутності технічної підтримки (неповнота документації, нестача довідкової інформації й т.ін.).

Основними джерелами внутрішніх відмов СППР є:

- відхід (випадковий або навмисний) від установлених правил експлуатації;
- вихід системи зі штатного режиму експлуатації в силу випадкових або навмисних дій користувачів або обслуговуючого персоналу (перевищення розрахункового числа запитів, надмірний обсяг оброблюваної інформації й т.п.);

- помилки при (пере) конфігуруванні системи;
- відмови програмного й апаратного забезпечення;
- руйнування даних;
- руйнування або ушкодження апаратури.

Стосовно підтримуючої інфраструктури рекомендується розглядати наступні загрози:

- порушення роботи (випадкове або навмисне) систем зв'язку, електроживлення, водо- і/або теплопостачання, кондиціювання;
- руйнування або ушкодження приміщень;
- неможливість або небажання обслуговуючого персоналу й/або користувачів виконувати свої обов'язки (громадянські непорядки, аварії на транспорті, терористичний акт або його загроза, страйк і т.ін.).

Досить небезпечні так звані «скривджені» співробітники – нинішні й колишні. Як правило, вони прагнуть завдати шкоди підприємству-кривднику, наприклад:

- зіпсувати обладнання;
- вилучити дані;
- вмонтувати закладку – «логічну бомбу», що згодом зруйнує програми й/або дані.

Скривджені співробітники, навіть бувші, знайомі з порядками в організації й здатні завдати чималої шкоди. Необхідно стежити за тим, щоб при звільненні співробітника його права доступу (логічного й фізичного) до інформаційних ресурсів вчасно анулювалися.

Небезпечні, зрозуміло, стихійні лиха й події – пожежі, повені, землетруси, урагани. Серед прикладів загроз доступності можна назвати ушкодження або навіть руйнування обладнання (у тому числі кабельних мереж, носіїв даних). Таке ушкодження може бути пов'язане з природними явищами, найчастіше – грозами. Існує міжнародний стандарт IEC 1312-1(02-1995) Protection against lighting electromagnetic impulse, що регламентує засоби захисту від цих загроз.

Небезпечними є також течія водопроводу й опалювальної системи. Такі випадки властиві приміщенням у будинках старої забудови; у сучасних серверних залах, дата-центрах це малоймовірно. Однак там можуть вийти з ладу кондиціонери, особливо влітку, у сильну спеку, що черевате значним збитком.

За статистикою на долю вогню, води й тому подібних «зловмисників» (серед яких найнебезпечніший – перебій електроживлення) приходиться до 10% втрат, нанесених системам. Тобто набагато частіше безпека страждає від людського дуру й безвідповідальності, ніж від стихійних лих.

Наступні загрози пов'язані з використанням у комп'ютерах довгострокової енергонезалежної пам'яті, тобто накопичувачів на жорстких магнітних дисках (НМЖД). Розміщення й зберігання інформації в таких пристроях створює передумови як для втрати важливої інформації, так і для несанкціонованого доступу до неї. Ще один приклад – умови зберігання резервних носіїв даних. Найчастіше їх зберігають недбало (це ще й загроза конфіденційності), не забезпечуючи їхній захист від шкідливого впливу навколишнього середовища. І коли потрібно відновити дані, ці самі носії можуть не читатися.

Однак найбільш істотні загрози доступності – програмні атаки на доступність. Як засіб виводу системи зі штатного режиму експлуатації може використовуватися агресивне споживання ресурсів (зазвичай – смуги перепуску мереж, обчислювальних можливостей процесорів або оперативної пам'яті). По розташуванню джерела загрози таке споживання підрозділяється на локальне й віддалене. При прорахунках у конфігурації системи локальна програма здатна практично монополізувати процесор і/або фізичну пам'ять, звівши швидкість виконання інших програм до нуля.

Віддалене негативне споживання ресурсів останнім часом проявляється в особливо небезпечній формі – як скоординовані розподілені атаки, коли на сервер з множини різних адрес із максимальною швидкістю направляються цілком легальні запити на з'єднання й/або обслуговування.

Основні загрози цілісності. Порушення цілісності інформації – це незаконне знищення або модифікація інформації. У якості джерел загроз цілісності знов треба казати про пожежі й стихійні лиха. Але тут також на першому місці за розмірами збитку – ненавмисні помилки й недогляди, випадкові й навмисні критичні ситуації в системі. На другому місці стоять крадіжки й підробки. За даними аналітичних агентств у результаті подібних протиправних дій з використанням комп'ютерів підприємствам наноситься загальний збиток у мільйони доларів. У більшості випадків винуватцями виявляються штатні співробітники підприємств, відмінно знайомі з режимом роботи й заходами з захисту. Це ще раз підтверджує небезпеку внутрішніх загроз.

Потенційно уразливі з погляду порушення цілісності не тільки дані, але й програми. Впровадження шкідливого ПЗ – причина подібного порушення. Зловредні програми – віруси, «троянські коні» і т.ін. дуже часто можуть призвести до знищення та модифікації інформації. У даних випадках зручніше казати про канали впливу на цілісність (або про канали руйнуючого впливу).

Основою захисту цілісності є своєчасне регулярне копіювання цінної інформації. Інший клас механізмів захисту цілісності заснований на ідеї

завадозахищеного кодування інформації (введення надлишковості в інформацію). Він заснований на автентифікації, тобто підтвердженні автентичності, цілісності інформації. Підтвердження автентичності охороняє цілісність інтерфейсу, а використання кодів автентифікації дозволяє контролювати цілісність файлів і повідомлень. Введення надлишковості в мови й формальне завдання специфікації дозволяє контролювати цілісність програм.

Нарешті, до механізмів контролю й захисту цілісності інформації варто віднести створення системної надлишковості. Такі заходи отримали назву підвищення «живучості» системи.

Живучість систем – це властивість складних систем адаптуватися до непередбачених ситуацій, протистояти небажаним впливам і виконувати мету функціонування за рахунок зміни поведінки і структури системи.

Але використання таких механізмів дозволяє не лише вирішувати завдання стійкості до помилок і захисту від порушень доступності і цілісності, але й дозволяє системі функціонувати при наявності небажаних впливів та їхньому накопиченні, зберігатися як цілому в екстремальних для неї умовах.

Існують загрози порушення цілісності електронних листів – заголовки можуть бути підроблені, лист у цілому може бути сфальсифіковано особою, що знає пароль відправника. Відзначимо, що останнє можливо навіть тоді, коли цілісність контролюється криптографічними засобами. Тут має місце взаємодія різних аспектів кібербезпеки: якщо порушено конфіденційність, може постраждати й цілісність.

Основні загрози конфіденційності. Конфіденційну інформацію, що обробляється в СППР, можна поділити на предметну й службову. Службова інформація, така, наприклад, як паролі користувачів, в СППР відіграє допоміжну технічну роль, але її розкриття є особливо небезпечним, оскільки це може мати наслідками одержання несанкціонованого доступу до всієї інформації, у тому числі предметної.

Експерти вважають, що існує тільки два шляхи порушення таємності (конфіденційності) – 1) втрата контролю над системою захисту; 2) наявність каналів витоку інформації.

Якщо система забезпечення захисту перестає адекватно функціонувати, то, природно, траєкторії процесу обробки інформації можуть пройти

через той стан, коли здійснюється заборонений доступ. Канали витоку характеризують ту ситуацію, коли або проектувальники не змогли попередити, або система не в змозі розгледіти такий доступ як заборонений. Втрата керування системою захисту може бути реалізованою оперативними заходами, й тут відіграють істотну роль адміністративні й кадрові методи захисту. Втрата контролю за захистом може виникнути в критичній ситуації, яка може бути створеною стихійно або штучно. Втрата контролю може виникнути й за рахунок виламування захисту самої системи захисту. Протиставити цьому можна тільки створення захищеного домену для системи захисту. Зрозуміло, у реальному житті використовуються й комбінації цих атак.

Канали витоку надають порушнику великі можливості. Тому використання СППР у військовій, державній і інших сферах діяльності, де переважно обробляється конфіденційна інформація, породжує ряд специфічних проблем, які необхідно вирішити для захисту інформації. Однією з них є виявлення можливих каналів витоку (просочування) інформації. Під можливим каналом витоку розумітимемо спосіб, що дозволяє порушникові отримати доступ до інформації, що обробляється або зберігається в системі.

Класифікацію можливих каналів витоку інформації в першому наближенні можна провести виходячи з типу засобу, що є основним при отриманні інформації по можливому каналу витоку. Слід розрізняти три типи таких засобів: людина, апаратура, програма. У відповідності до кожного типу засобу усі можливі канали витоку також розбиваються на три групи.

Стосовно людини можливі наступні канали витоку:

- розкрадання носіїв інформації;
- читання інформації з екрану сторонньою особою (наприклад, під час відображення інформації на екрані законним користувачем або у відсутність його на робочому місці);
- читання інформації із залишених без нагляду роздруківок (текстів, програм. тощо).

У групі апаратних каналів витоку можна виділити такі шляхи витоку:

- підключення до обладнання АРМ спеціально розроблених апаратних засобів, що забезпечують доступ до інформації;
- використання спеціальних технічних засобів для перехоплення електромагнітних випромінювань технічних засобів АРМ.

У групі каналів, в яких основний засіб забезпечення витоку – програма, можна виділити такі основні шляхи витоку:

- несанкціонований доступ програми до інформації;
- розшифрування програмою зашифрованої інформації.

Основні класи каналів витоку в СППР – це так звані *канали по пам'яті* та *канали за часом.* Канали по пам'яті – це канали, які утворюються за рахунок використання доступу до загальних об'єктів системи.

У директорію О внесені імена файлів. Хоча доступ до самих файлів для суб'єкта S_1 закритий, доступ до директорії O є можливим. Тоді якщо суб'єкт S_2 створив закриті файли, то інформація про наявність цих файлів стала доступної S_1. Відбувся витік частини інформації.

Канал за часом є каналом, що передає порушнику інформацію про процес, модульований цінною закритою інформацією. Захисні механізми від таких каналів засновані на контролі інформаційних потоків у системі.

Нехай процес S_a використовує принтер для друку результатів чергового циклу обробки інформації. Процес $S_в$ визначається роботою принтера, який є загальним ресурсом користувачів U_1 і U_2 із пріоритетом у U_2. Процес $S_в$ регулярно із заданою частотою надсилає запит на використання принтера й отримує відмову, коли S_a роздруковує чергову порцію інформації. Тоді в одиницях частоти запиту користувач U_1 отримує інформацію про періоди обробки процесом S_a цінної інформації, тобто маємо канал витоку.

Ще одним прикладом каналу витоку за часом є перехоплення інформації в каналі зв'язку. Тут реалізується безпосередній доступ до процесу обробки (передачі) цінної інформації. Знімання інформації про цей процес і нагромадження її в часі відновлюють передану цінну інформацію. Захист від цих каналів засновується на криптографії (шифруванні інформації). Типовими каналами витоку за часом є й побічні канали витоку по електромагнітному випромінюванню, по електроживленню або акустиці. Захисні механізми тут мають засновуватись на екрануванні, фільтрах і зашумленні.

Описаний клас уразливих місць можна назвати розміщенням конфіденційних даних у середовищі, у якому їм не забезпечений необхідний захист. Загроза ж полягає у тому, що завжди хтось не відмовиться довідатися про секрети, які самі просяться в руки. Крім паролів, що зберігаються на аркушах паперу, у цей клас попадає передача конфіденційних даних у відкритому виді (у розмові, у листі, по мережі), що уможливлює перехоплення даних. Для атаки можуть використовуватися різні технічні засоби (підслуховування або прослуховування розмов, пасивне прослуховування мережі й т.п.), але ідея одна – здійснити доступ до даних у той момент, коли вони найменш захищені.

Загрозу перехоплення даних варто брати до уваги не тільки при початковому конфігуруванні СППР та її стаціонарному функціонуванні, але й, що дуже важливо, при всіх змінах, що вносяться у систему.

Ще один приклад – зберігання даних на резервних носіях. Для захисту даних на основних носіях застосовуються розвинені системи керування доступом; копії ж нерідко просто лежать у шафах і одержати доступ до них можуть багато хто.

Перехоплення даних – дуже серйозна загроза, і якщо конфіденційність дійсно є критичною, а дані передаються по багатьом каналам, їхній захист може виявитися досить складним й дорогим. Технічні засоби перехоплення добре пророблені, доступні, прості в експлуатації, а встановити їх, наприклад, на кабельну мережу, може хто завгодно, так що цю загрозу потрібно брати до уваги по відношенню не тільки до зовнішніх, але й до внутрішніх комунікацій.

Наступні загрози пов'язані з використанням у комп'ютерах довгострокової енергонезалежної пам'яті, тобто накопичувачів на жорстких магнітних дисках (НМЖД). Один з каналів витоку – *можливість відновлення вилученої інформації* на дисках, наприклад, направлених на ремонт або зданих в утиль. Можливість відновлення інформації заснована на тому, що при стиранні інформації засобами операційної системи фактично стираються тільки дані про розташування інформації на диску, а сама інформація фізично не знищується.

Крадіжки обладнання є загрозою не тільки для резервних носіїв, але й для комп'ютерів, особливо портативних. Часто ноутбуки залишають без догляду на роботі або в автомобілі, іноді просто втрачаються.

Небезпечною нетехнічною загрозою конфіденційності є методи морально-психологічного впливу, такі як «маскарад» – виконання дій під видом особи, що має повноваження для доступу до даних.

До неприємних загроз, від яких важко захищатися, можна віднести зловживання повноваженнями. На багатьох типах систем привілейований користувач (наприклад системний адміністратор) здатний прочитати кожний (незашифрований) файл, отримати доступ до пошти будь-якого користувача й т.ін. Інший приклад – завдання збитків при сервісному обслуговуванні. Звичайно сервісний інженер отримує необмежений доступ до обладнання й має можливість діяти поза програмними захисними механізмами.

1.2.3. Шкідливе програмне забезпечення

Розглянувши найпоширеніші загрози доступності, цілісності та конфіденційності не можна не зазначити, що одним з найнебезпечніших способів проведення атак є запровадження в системи, що атакуються, *шкідливого програмного забезпечення*. Джерела та можливі шляхи його поширення, а також напрямки атак є дуже різноманітними (рис. 1.8).

	**Шкідливе програмне забезпечення** *(malware)* – програмний код, що виконується або інтерпретується, який має властивість несанкціонованого поширення й самовідтворення в автоматизованих системах або телекомунікаційних мережах з метою змінити або знищити програмне забезпечення й/або дані, що зберігаються в автоматизованих системах.

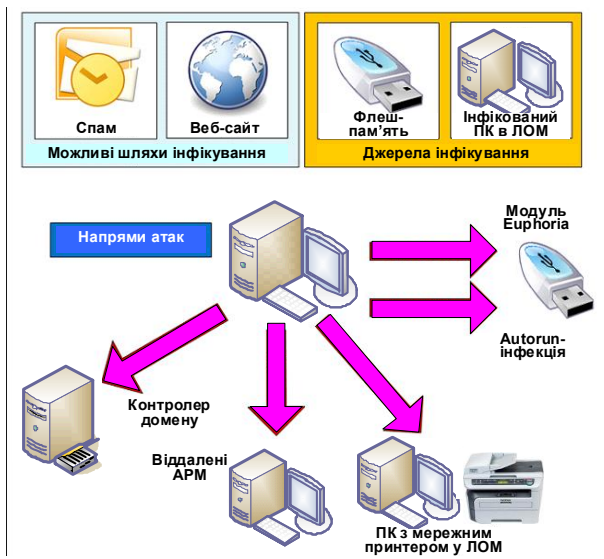


Рис. 1.8. Джерела, можливі шляхи поширення та напрямки атак шкідливого програмного забезпечення

Виділимо наступні грані шкідливого ПЗ:

- шкідлива функція;
- спосіб поширення;

- зовнішнє представлення.

Спектр шкідливих функцій можна вважати необмеженим, оскільки шкідливе ПЗ, як і будь-яка інша програма, може мати як завгодно складну логіку. Зазвичай шкідливе ПЗ призначається для:

- впровадження іншого шкідливого ПЗ;
- одержання контролю над системою, що атакується;
- агресивного споживання ресурсів;
- зміни або руйнування програм і/або даних;
- збирання та передачі інформації з зараженого комп'ютера.

Шкідливе програмне убезпечення класифікують за різними ознаками. По-перше, в деяких джерелах шкідливе програмне забезпечення виділяють як так звані програмні закладки (program bug). Програмна закладка – це засіб, що працює на комп'ютері деякий час, допоки його не буде виявлено, або у відповідності до алгоритму його роботи. Таким чином це визначення не можна вважати коректним, адже будь-яка шкідлива програма може або встановлювати програмну закладку, або не робити цього.

За іншими джерелами шкідливе ПЗ поділяють на дві категорії – таке, що виконує деструктивні (руйнівні) функції, і таке, що їх не виконує. Тут також є неоднозначність, адже навіть якщо розробник шкідливого засобу не передбачив у ньому руйнівних функцій, такий засіб може призвести до значних втрат – як через необхідність спрямування зусиль висококваліфікованих (і високооплачуваних) фахівців на виявлення, ідентифікацію та видалення шкідливого програмного засобу, так і через недоступність системи.

Більш доречним, з огляду на забезпечення безпеки СППР, є класифікація шкідливого ПЗ за такими двома ознаками:

- за способом розповсюдження засобу, тобто яким чином засіб потрапляє у систему і домагається своєї активізації;
- за метою функціонування засобу, тобто які саме шкідливі дії він здійснює у системі.

Шкідливе програмне забезпечення завдає капостив комп'ютеру під час запуску його коду на виконання. Ці засоби застосовують такі механізми розповсюдження, що дають їм змогу виконуватися на комп'ютері або взагалі без втручання користувача, або непомітно для нього. Тому за механізмами розповсюдження поділяють шкідливі програмні засоби на класичні комп'ютерні віруси (файлові віруси; завантажувальні віруси; макровіруси; скрипто-віруси), мережні хробаки (поштові хробаки; хробаки для файлообмінних мереж; хробаки в IRC-каналах; інші), «троянські коні», програмні закладки, а також спеціальні засоби.

Віруси – це код, що має здатність до поширення (можливо, зі змінами) шляхом впровадження в інші програми. Віруси звичайно поширюються локально, у межах вузла мережі; для передачі по мережі їм потрібна зовнішня допомога, така як пересилання зараженого файлу.

«Хробаки» – це код, здатний самостійно, тобто без впровадження в інші програми, викликати поширення своїх копій по системі і їхнє виконання (для активізації вірусу потрібен запуск зараженої програми). Тому хробаки, навпроти, орієнтовані в першу чергу на подорожі мережами. Іноді саме поширення шкідливого ПЗ викликає агресивне споживання ресурсів і, отже, є шкідливою функцією. Наприклад, хробаки «з'їдають» смугу перепуску мережі й ресурси поштових систем, що можна віднести до атак на доступність.

Іноді хробаками називають також такі програми, які не здатні самотужки запустити себе на виконання на віддаленій системі, й відтак застосовують принцип «троянського коня». Шкідливий код, що виглядає як функціонально корисна програма, ***називається троянським***. Наприклад, звичайна програма, будучи ураженої вірусом, стає троянською.

Щодо способу зараження комп'ютера, то про нього каже сама назва «троянський кінь». Ці програми, використовуючи різні методи соціальної інженерії, приваблюють довірливого користувача, який запускає їх на виконання, отримуючи зовсім не ті результати, на які розраховував (у деяких «троянських коней» шкідливі функції добре приховано, тому користувач може навіть не підозрювати, що його комп'ютер уже скомпрометовано). Так, відомі програми, що використовується для вимагання викупу. Для того, щоб запобігти вилученню, цей засіб побудований з використанням криптографії. Він знає свій відкритий ключ, таємний ключ відомий автору програми. «Троян» проникає у комп'ютер, використовуючи відкритий ключ, шифрує необхідні дані і передає авторові. Після цього інформує користувача, що його комп'ютер заражений і пропонує зв'язатися з автором. Той, у свою чергу, потребує викупу. У разі несплати вірус може нанести непоправної шкоди.

Повернемося до вірусів. ***Файлові віруси*** для свого розповсюдження використовують файлову систему. Найчастіше віруси цього типу як носій застосовують виконувані файли. Крім виконуваних файлів віруси заражають об'єктні модулі ((OBJ), бібліотеки компіляторів (LIB), інсталяційні пакети і вихідні тексти програм. Є віруси, які записують свої копії в архіви (ARJ. ZIP, RAR), а є й такі, що для розповсюдження копіюють свій код у певні каталоги на дисках, сподіваючись на те, що користувач колись запустить їх.

Завантажувальні віруси, або бутові (*boot* – початкове завантаження, комп'ютерний термін, скорочення від Bootstrap Loader – програма початкового завантаження) активуються у момент завантаження системи. Дія цього їм потрібно розташувати частину свого коду в службових структурах носія, з якого відбувається завантаження, зазвичай це жорсткий диск. Зараження жорсткого диска відбувається в один із трьох способів: 1) вірус записує себе замість коду MBR (Master Boot Record – головний завантажувальний запис, таблиця у першому секторі завантажувального диска, 2) вірус записує себе замість коду boot-сектора завантажувального диска (у Windows це, як правило, диск C) або 3) модифікує таблицю активного boot-сектора в таблиці розділів диска (Disk Partition Table), що знаходиться в MBR. Бутові віруси можуть дуже ефективно протистояти антивірусним засобам, оскільки саме віруси стартують першими, ще до запуску операційної системи, і тому вони здатні залишити за собою керування критичними для їх існування ресурсами комп'ютера, зокрема, файловою системою.

Макровіруси – це віруси, які використовують прихований у файлах документів програмний код (так звані макроси). Свої макромови (множина передбачених у програмі оброблення документа макрокоманд) мають графічні редактори, системи автоматизованого проектування, текстові та табличні процесори. Макровіруси також написано макромовами. Передумови для макровірусів виникли, коли з'явилися можливості зберігання макросів у файлі документа. Крім того, макроси мають доступ не лише до документа, в якому вони містяться, а й до файлової системи. Усе це й створило основу дія розроблення та розповсюдження вірусів.

Макровіруси зазвичай вражають файли Micrоsoft Office шляхом перевизначення стандартних системних макросів або автоматично запускаються після виконання певної умови (натис-кання клавіші або кількох клавіш, настання визначеного моменту часу). Отримавши керування, макровірус впроваджує свій код в інші файли, частіше у відкриті для редагування, рідше – самостійно шукає файли на диску. Файли документів розповсюджуються на знімних носіях, пересилаються електронною поштою, тим самим створюється підґрунтя для поширення вірусів.

Програмний код впроваджують і в документи інших видів, наприклад в HTML-сторінки, що завантажуються з Інтернету та відображаються на екрані за допомогою браузера. Наразі автоматично виконується програмний код сценаріїв, які ще називають скриптами (script-сценарій) та інших елементів (ActivX, Java). ***Скриптові віруси*** розглядають як підгрупу файлових вірусів (так звані ***мобільні агенти***). Вони можуть заражати

інші програми-сценарії, бути компонентами багатокомпонентних вірусів, заражати файли інших форматів, якщо вони підтримують виконання сценаріїв.

До ***спеціальних засобів*** належать дуже небезпечні засоби, які не мають своїх механізмів розповсюдження і які користувачі свідомо запускають на виконання як звичайні програми. Такі засоби зловмисники застосовують, якщо мають певні повноваження в системі (можливо, отримані несанкційовано). Деякі з цих засобів називають експлойтами (exploit), що підкреслює факт використання (експлуатації) ними деякої вразливості системи. Експлойти використовуються для організації автоматичних «drive-by» атак з метою поширення шкідливого ПЗ. Часто такі засоби призначені для атаки не того комп'ютера, на якому вони виконуються, а інших комп'ютерів у мережі (рис. 1.9).

Рис. 1.9. Схема дії експлойту

Також популярними є хакерські інструменти руткіти (rootkit). Ця назва прийшла з операційної системи UNIX, де її використовували для позначення набору інструментів, що застосовували для отримання прав суперкористувача з ім'ям root. До такого набору обов'язково входили засоби, що давали змогу впроваджувати люк і приховувати його присутність у системі. Тепер цю назву використовують для програмного коду або технології, спрямованої на приховування присутності в системі заданих об'єктів (процесів, файлів, ключів реєстру тощо).

Ще один клас програмного забезпечення, використання якого може призвести до пошкодження програмного, а інколи навіть апаратного забезпечення системи – це *технологічні програми* (утиліти), які використовують адміністратори системи або технічний обслуговуючий персонал, наприклад, засоби резервного копіювання і відновлення з резервних копій, форматування дисків, дефрагментації файлових систем, та ін.

Технологічні програми не належать до шкідливих чи руйнівних, проте, оскільки їх використання зловмисниками або просто некомпетентними користувачами може мати дуже серйозні наслідки, це слід враховувати і передбачати заходи, що запобігають їх шкідливому використанню.

Програмні закладки – це програми або окремі функції програм, що тривалий час працюють у системі, виконуючи дії, спрямовані на приховування свого існування від користувача. Програмні вкладки можуть впроваджувати віруси, «троянські коні», хробаки чи безпосередньо користувачі-зловмисники.

Функцій програмних закладок досить різноманітні. Вони зокрема полягають у перехопленні і передаванні інформації, порушенні функціонування системи, модифікації програмного забезпечення, здійсненні психологічного тиску на користувача, тощо.

До небезпечних закладок слід віднести так звані «логічні бомби» та «люки». До категорії ***«логічних бомб»*** належать програмні закладки, які за певних умов здійснюють руйнівні дії. Серед них виокремлюють категорію «часових бомб», де умовою запуску є настання певного моменту часу.

«Люки» є утилітами віддаленого адміністрування комп'ютерів у мережі. Функціонально вони подібні до систем адміністрування, що постачають відомі виробники програмних продуктів. Єдине, що відрізняє закладки – це відсутність попереджень про їх інсталяцію і запуск. «Люки» використовуються зловмисниками для інсталяції на комп'ютерах своїх утиліт-ботів, що перетворює їх на машини-зомбі. Скомпрометовані комп'ютери стають учасниками деякого ботнета (botnet, від robot і network), або навіть кількох таких зловредних угруповань (рис. 1.10).

Ботнети використовуються для організації атак на віддалені сервери, так званих DoS- і DDoS-атак. DoS-атаки – це атаки на відмову в обслуговуванні (Denial of Service, DoS), загроза яких полягає в тому, що на сервер надсилають так багато запитів, скільки дозволяють ресурси зловмисника. Мета досягається, коли можливості сервера не дозволяють

опрацювати усі запити, що надходять. DDoS-атаку (Distributed DoS) організовують з багатьох комп'ютерів одночасно, тому шансів на успіх у зловмисників набагато більше.

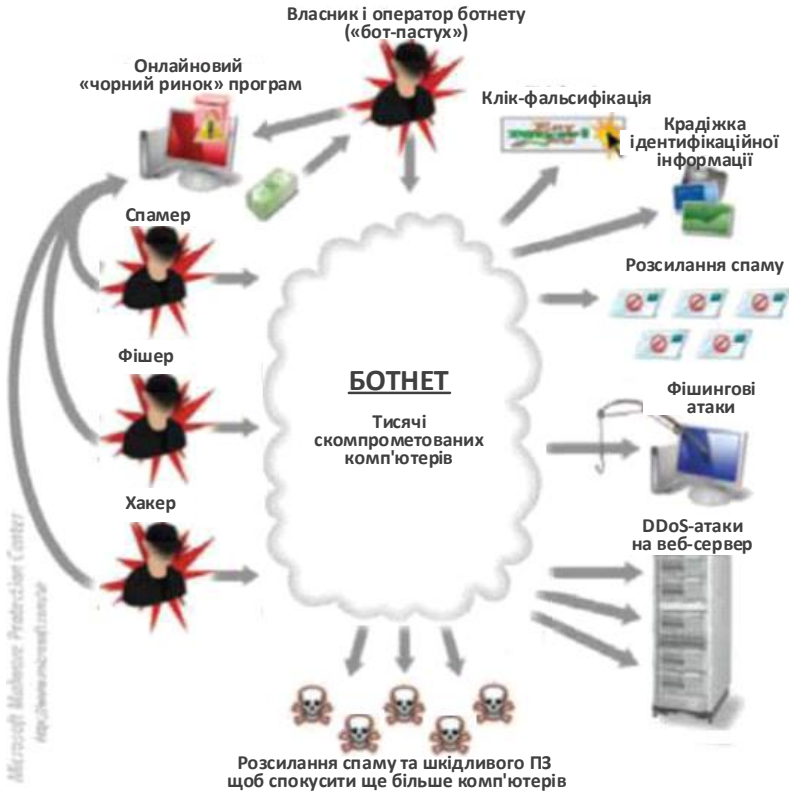


Рис. 1.10. Схема формування ботнету

Програмні закладки, що відслідковують усі дії на комп'ютері, здійснюють пошук інформації на зараженому комп'ютері та передають її зловмиснику, отримали назву ***шпигунські програми*** (spyware). Є два їх різновиди. Перші поцуплюють інформацію і паролі. Наприклад, здійснюють пошук інформації у файлах користувача за певними ознаками (приміром, за ключовими словами). Інші – протоколюють дії з клавішами клавіатури і передають ці протоколи розробнику програми. Можуть мати вигляд «бомби», коли тихо сплять і уводяться в дію за командою ззовні.

Нарешті, дуже популярним стало використання соціальних методів, зокрема тактик обману, схожих на маркетингові акції, рекламного програмного забезпечення (adware), фішингу (phishingt) з використанням соціальних мереж для заманювання користувачів, а також застосування шахрайського ПЗ для забезпечення безпеки, що має назву «scareware» (від scare – лякати).

На завершення слід зазначити, що вікно небезпеки для шкідливого ПЗ з'являється з випуском нового різновиду вірусів і/або хробаків і перестає існувати з відновленням бази даних антивірусних програм і накладенням інших необхідних латок.

Водночас можна стверджувати, що дотримання нескладних правил «комп'ютерної гігієни» практично зводить ризик зараження вірусами до нуля. Треба, перш за все, не відкривати приєднані файли, що поширюються від невідомих джерел за допомогою електронної пошти, не скачувати програми з сумнівних сайтів, взагалі не відвідувати такі сайти.

Із цього приводу слід звернути увагу на два моменти.

1. Пасивні об'єкти відходять у минуле, а нормою стає активний вміст. Файли, які за всіма ознаками повинні були б відноситися до даних, тобто бути пасивними об'єктами (наприклад, документи у форматах MsWord, тексти поштових повідомлень), здатні містити компоненти, що інтерпретуються, які можуть запускатися неявним способом при відкритті файлу.

2. Інтеграція різних сервісів, наявність серед них мережних, загальна зв'язність, зокрема з використанням Інтернету, багаторазово збільшують потенціал для зловмисних атак, полегшують поширення шкідливого ПЗ.

Протидією шкідливому ПЗ є так зване антивірусне програмне забезпечення. Особливості його створення та використання будуть розглянуті у подальших розділах курсу.

Контрольні запитання та завдання

1. Дайте визначення поять атака, порушник, джерело загрози.
2. Дайте визначення поять уразливість, вади захисту, вікно небезпеки.
3. Представте структуру опису моделі загроз та моделі порушника.
4. За якими основними критеріями можна класифікувати загрози?
5. Категорії методики класифікації загроз STRIDE.
6. Назвіть найпоширеніші загрози цілісності і доступності для СППР.

7. Що таке живучість систем?
8. Наведіть приклади можливих каналів витоку в СППР.
9. Назвіть грані шкідливого ПЗ.
10. Дайте характеристики експлойту та ботнету.
11. Що таке шпигунські програми?

1.3. ТЕОРЕТИЧНА ТА МЕТОДОЛОГІЧНА БАЗА ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

Загальнотеоретичне уявлення вирішення проблем кібербезпеки.
Основні традиційні підходи до інформаційної безпеки, їх переваги та недоліки.
Об'єктно-орієнтований підхід.
Систематизований підхід

1.3.1. Загальнотеоретичне уявлення вирішення проблем кібербезпеки

Питання забезпечення інформаційної та кібербезпеки в наші часи стрімкого розвитку інформаційних технологій та формування інформаційного суспільства стають усе більш актуальними. Тому у сферу вивчення та реалізації цих питань утягується усе більше фахівців та науковців не лише з інформаційних технологій, а й з багатьох різних галузей та сфер діяльності.

Це обумовлено тим, що питаннями безпеки взагалі як однієї з соціальних проблем людства займаються чимало людей. А проблема інформаційної безпеки проникає у всі інші сфери безпеки (економічної, соціальної, оборонної, тощо) та поступово виходить на передній план.

Побудова систем захисту інформації (СЗІ) пов'язана з багатьма специфічними особливостями, до яких слід віднести:

- неповнота й невизначеність вихідної інформації про состав АС і її характеристики, а також про характерні загрози;
- багатокритеріальність завдання, пов'язана з необхідністю обліку великої кількості часткових показників (вимог) АС та СЗІ;
- наявність як кількісних, так і якісних показників, які необхідно враховувати при розв'язанні завдань розробки й впровадження СЗІ;
- неможливість застосування класичних методів оптимізації.

Внаслідок цього склалася ситуація, коли чимало підприємств на власний розсуд вирішують завдання забезпечення кібербезпеки й залучає для цього різних фахівців, які застосовують свої способи й методи для досягнення заданих цілей. При цьому, навіть якщо й знаходяться достатньо вірні рішення, часто-густо система безпеки в цілому працює не ефективно. Таке становище обумовлене відсутністю загальновизнаного системного підходу, що визначав би взаємні зв'язки між існуючими поняттями, принципами і способами використання механізмів захисту та побудови систем безпеки. З іншого боку важливою проблемою є проблема складності вивчення (аналізу) СЗІ. Нарешті, ще однією проблемою є побудова (синтез) *гарантовано захищеної* системи.

Різноманіття варіантів побудови систем підтримки прийняття рішень породжує необхідність створення різних систем захисту, що враховували б індивідуальні особливості кожної з СППР. Виникає питання: чи можна сформувати такий підхід до створення систем захисту інформації, який, з одного боку, був би універсальним, простим, зрозумілим, об'єднав би в єдине ціле наявні знання й досвід у сфері безпеки, а з іншого боку – дозволяв би однаковою мірою задовольнити будь-які вимоги й характеристики, властиві тільки даній конкретній автоматизованій системі?

Звісно, спроби визначити такий підхід в сфері кібербезпеки постійно ведуться. Основою цього пошуку є *теорія захисту інформації*, яка являє фундаментальне підґрунтя такої сфери звань як захист інформації.

Теорія захисту інформації – це наука про загальні принципи та методи побудови захищених інформаційно-комунікаційних систем.

Теорія захисту інформації – це природнича наука, яка має відповідні аксіоматику, понятійний та формальний апарат. Її основним методологічним інструментом є методи системного аналізу для вивчення складних систем і теорія прийняття рішень, що застосовуються для розв'язання задач синтезу систем захисту інформації та визначення таких категорій, як *політика безпеки* та *критерій безпеки*.

Політика безпеки *(security policy)* – набір законів, правил і практичного досвіду, на основі яких будується управління, захист і розподіл критичної інформації.

Критерій безпеки – всебічна порівняльна оцінка стану безпеки людини, суспільства, держави й довкілля з погляду найважливіших про-

цесів, явищ, параметрів, що відображають її суть. Критерій є якісною оцінкою, на основі якої адекватно визначається рівень безпеки.

Критерій безпеки інформації – показник, що характеризує безпеку інформації при дії різних чинників небезпеки.

Загальнооб'єднуючим в створенні механізмів захисту інформації, що компонуються в єдиний цілісний механізм – систему захисту інформації, є поняття *системності*. Воно представляється як регулярний процес, що реалізується на всіх етапах життєвого циклу АІС. Практичне вирішення вказаного питання полягає в розробці на основі науково-методичного апарата *моделей безпеки та представлення системи (процесів) забезпечення безпеки,* що дозволяли б вирішувати не тільки завдання створення СЗІ для проектованих і існуючих унікальних АС, а й для оцінки їхньої ефективності.

Наразі в теорії захисту інформації для визначення цих категорій, аналізу та синтезу систем використовують два підходи – *формальний* і *неформальний*. Традиційно формальний підхід полягає у визначенні політики безпеки, критерію безпеки та моделі безпеки АС у формальному вигляді. За формального підходу необхідно довести відповідність системи безпеки АС критерію безпеки за умови дотримання встановлених правил і обмежень. У цьому разі говорять про «гарантованість» захисту інформації. Побудова (синтез) гарантовано захищеної системи є однією з проблем теорії захисту. В класі відкритих систем цю проблему відносять до алгоритмічно нерозв'язних проблем. Доказове обґрунтування відсутності гарантовано захищених систем надає у праці М. Харрісона, В. Руззо, Дж. Ульмана «Захист в операційних системах» (1976р.) теорема про унеможливлення розв'язання задачі гарантування безпеки довільної відкритої системи.

Підходи до вирішення проблем аналізу і синтезу систем гарантованого захисту інформації, що у 80-х роках минулого століття було впроваджено в документі «Критерії оцінки захищених комп'ютерних систем» (*«Trusted Computer System Evaluation Criteria», TCSEC*) Міністерства оборони США, відомого як «Оранжева книга», є теоретичним базисом багатьох сучасних стандартів захисту інформації. Ці підходи узагальнюють досвід розвитку теорії захисту інформації, який поетапно вище було відображено в табл. 1.3.

За цією таблицею методологічно етапи розвитку теорії захисту інформації розрізняються наступним чином. Емпіричний період розвитку характеризується використанням неформальних (описових) методів для вирішення завдань аналізу систем захисту інформації, коли синтез систем

захисту здійснювався методом проб та помилок, на основі використання функціонально орієнтованих механізмів захисту. Другий період, що характеризується використанням концептуально-емпіричного підходу, відрізняється від попереднього певним узагальненням неформальних підходів до аналізу систем захисту інформації. Синтез систем захисту інформації здійснювався із застосуванням уніфікованих та стандартних рішень із захисту.

Теоретико-концептуальний період вже характеризується використанням для вирішення завдань аналізу методів формальної теорії. Завдання синтезу систем захисту інформації вирішуються з використанням математичних теорій оптимізації, системного аналізу, прийняття рішень.

Формальний підхід теорії захисту інформації перебуває на стадії становлення і не може задовольнити всі вимоги, що виникають під час дослідження та створення систем захисту інформації. Тому цей підхід доповнюється традиційним неформальним (описовим) підходом.

Неформальний підхід являє собою опис методів і механізмів, які використовують дія захисту інформації в АС. У теорії захисту інформації цю проблему вирішують, застосовуючи метод ієрархічної декомпозиції складних систем, коли загальну складну систему розподіляють на ієрархічні рівні (рис. 1.11). Вказані підсистеми вивчають із застосуванням характерних для кожного рівня методів аналізу.

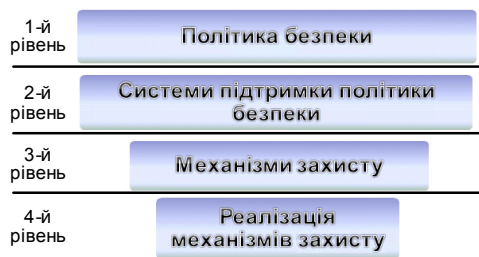


Рис. 1.11. Ієрархічна декомпозиція системи захисту

Слід зазначити, що який би підхід не застосовувався, методи досліджень систем захисту зазвичай зводяться до класичної побудови моделей об'єкту або внесення в об'єкт дослідження деякої структури, що має штучний характер, але полегшує дослідження. Так, наприклад, для опису й аналізу загроз інформації вноситься *структура інформаційного потоку.* У свою чергу структура *цінності інформації* дозволяє зрозуміти, що треба і що не треба захищати, а якщо захищати, то якою ціною.

На рис.1.12 у спрощеному виді представлені чинники, що впливають на побудову такої моделі.

Рис. 1.12. Чинники, що впливають на побудову моделі системи захисту

Отже, основним завданням моделі безпеки є науково обґрунтоване забезпечення процесу створення системи кібербезпеки за рахунок правильної оцінки ефективності прийнятих рішень і вибору раціонального варіанта технічної реалізації СЗІ.

	Головне ж, що витікає з досвіду розвитку методологій, це те, що підходи до ІБ необхідно аналізувати з точки зору рівня розгляду проблеми.

1.3.2. Основні методологічні підходи до розгляду проблем кібербезпеки

У якості методологічної бази розгляду проблем кібербезпеки напрацьовано кілька підходів, а саме: традиційний (суб'єкт-об'єкт); процесний; об'єктно-орієнтований.

До найбільш загальних підходів відноситься **процесний підхід**. Він притаманний сучасному уявленню про функціонування підприємства та інформаційних систем (рис. 1.13, 1.14). Процесний підхід описаний в стан-

дарті ISO 9001:2000 й міцно увійшов у життя багатьох компаній в усьому світі, де він використовується, наприклад. для опису бізнес-процесів. Процесний підхід розглядає проблеми на високому рівні та базується на інфраструктурі і ресурсах АІС.

	**Процес** *(process)* – сукупність організаційних елементів, відношень, ресурсів, що розглядаються у динаміці.

Рис. 1.13. Уявлення процесу

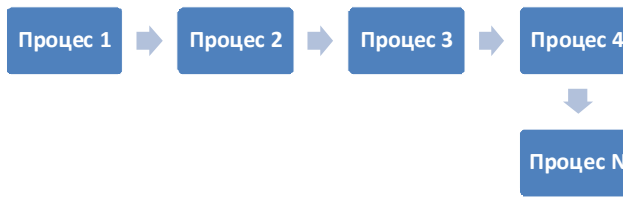


Рис. 1.14. Процесне уявлення системи

Зручність цього підходу полягає також у тому, що стає можливим контролювати проходження кожного процесу (рис. 1.15), чим забезпечується й контрольованість функціонування системи. Тому процесний підхід є основою забезпечення управління (менеджменту) кібербезпеки.

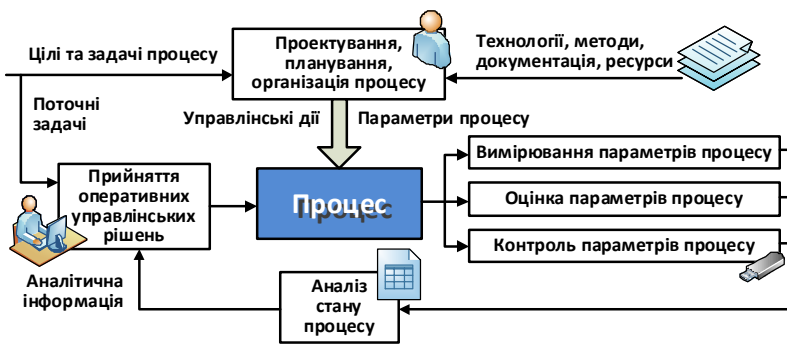


Рис. 1.15. Схема контролю процесу у системі

На рис. 1.16 наведено структуру процесів забезпечення кібербезпеки за так званою схемою PDCA (Plan, Do, Chek, Akt), тобто (Планування заходів з безпеки, Впровадження заходів, Перевірка їх ефективності, Покращення заходів). На рис. 1.17 наведено більш детальну схему циклічного процесу керування безпекою.

	Забезпечення кібербезпеки та управління кібербезпекою є безперервним циклічним процесом.

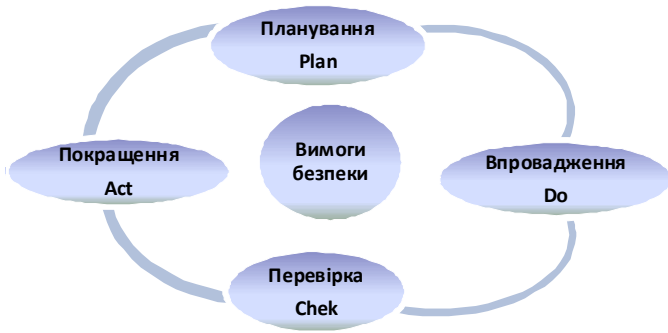


Рис. 1.16. Структура процесів забезпечення кібербезпеки за схемою PDCA

Рис. 1.17. Складові управління кібербезпекою у безперервному процесі

Перевагами процесного підходу є простота і прозорість, ефективне використання ресурсів, єдине розуміння на всіх рівнях. Недоліки ж по-

в'язані з труднощами впровадження цього підходу, пов'язані із складністю з визначенням чіткої інтеграції процесів в єдину систему з-за значної їх кількості, проблематичністю дотримання інтересів всіх учасників ланцюжка процесів, різними тлумаченнями й розумінням стандарту у різних консультантів (експертів).

Досвід вказує, що процес ний підхід «запрацює» тільки в умовах створення системи збалансованих показників в галузі безпеки. Але це дуже не просто, особливо з огляду на те, що система управління (менеджменту) інформаційної безпеки поки знаходиться більше в області теорії й концепції, а не успішної практики.

Підхід «суб'єкти й об'єкти» відноситься до традиційного, адже у звичній для сфери безпеки термінології на рівні процесів існує поділ на активні й пасивні сутності, тобто на ***суб'єкти*** й ***об'єкти***.

Розглянемо приклади. Об'єктом є довільний файл у комп'ютері. У будь-який момент у файл може бути щось записане. Файл є пасивною сутністю. Тепер нехай текст у файлі буде поділений на певні розділи. Будь-який такий розділ також є об'єктом. Таким чином, один об'єкт може бути частиною іншого. Ще приклад. Принтер – це об'єкт. Множина припустимих станів принтера є кінцевою. Саме ця кінцева множина і визначає принтер як об'єкт.

Розрізняють активні об'єкти і пасивні об'єкти. Активні об'єкти можуть виконувати дії над пасивними об'єктами. До активних об'єктів відносяться: 1) об'єкти-користувачі; 2) об'єкти-процеси.

У більшості зарубіжних стандартів пасивні об'єкти називають ***об'єктами*** (object), а активні об'єкти – ***суб'єктами*** (subject). Потрібно розуміти, що, як правило, суб'єкт – це об'єкт-процес, який діє від імені певного об'єкта-користувача.

Об'єкт-користувач *(user object)* – це подання фізичного користувача в обчислювальній системі, яке утворюється під час його входження в систему і характеризується своїм контекстом (обліковий запис, псевдонім, ідентифікаційний код, повноваження тощо).

Об'єкт-процес *(process object)* – задача, процес, потік, що виконується в поточний момент (абстракція програми, що виконується) і повністю характеризується своїм контекстом (стан регістрів, адресний простір, повноваження тощо).

З точки зору безпеки інформації в АС виняткове значення має спроможність об'єктів взаємодіяти. Для цього використовують поняття ***доступу*** (рис. 1.18).

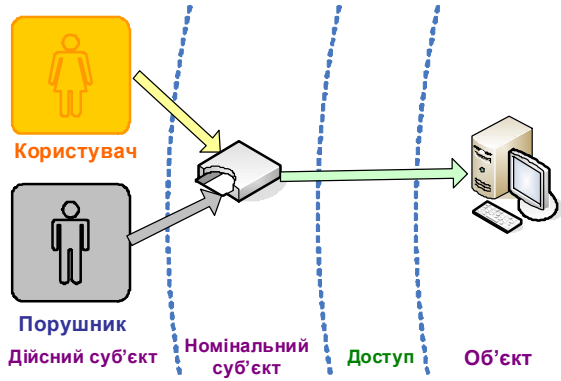


Рис. 1.18. Поняття доступу

Результатом доступу є утворення інформаційного потоку від одного об'єкта до іншого (наприклад, читання або записування інформації). У випадку, коли утворюється інформаційний потік, кажуть, що здійснюється *доступ до інформації*. Для забезпечення захисту інформації доступ до об'єктів, які містять інформацію, що підлягає захисту, слід здійснювати з дотриманням визначених правил, зокрема правил розмежування доступу.

	Доступ *(access)* – це взаємодія двох об'єктів обчислювальної системи, коли один із них (той, що здійснює доступ) виконує дії над іншим (тим, до якого здійснюється доступ).

	В розгляді питань захисту інформації приймається аксіома, яка покладена в основу американського стандарту із захисту (так званої «Оранжевої книги»). Її можна сформулювати в наступній формі: *всі питання безпеки інформації описуються доступами суб'єктів до об'єктів.*

Цей термін є найбільш уживаним, переважно до систем, в яких обробляють конфіденційну інформацію, тому його винесено в назви деяких нормативних документів системи технічного захисту інформації (НД ТЗІ). Разом із тим у цих документах зазначено, що захист інформації не обмежується захистом від НСД.

В системах існує множина різних видів доступів. Прийнято множину можливих доступів у системі позначати ***R***. Множина об'єктів позначається через ***O***, а множина суб'єктів – ***S***.

Правила розмежування доступу (ПРД) *(access mediatorien rules)* – складова політики безпеки, що регламентує правила доступу користувачів і процесів до пасивних об'єктів.

Несанкціонований доступ (НСД) *(unauthorized access)* – доступ, який здійснюють з порушенням політики безпеки, тобто з порушенням ПРД.

Розглянемо деякі основні приклади доступів.

1. Доступ суб'єкта *S* до об'єкта *O* на читання *(r)* даних в об'єкті *O*.

При цьому доступі дані зчитуються в об'єкті *O* и використаються як параметр у суб'єкті *S*.

2. Доступ суб'єкта *S* до об'єкта *O* на запис *(w)* даних в об'єкті *O*.

При цьому доступі деякі дані процесу *S* записуються в об'єкт *O*. Тут можливе стирання попередньої інформації.

3. Доступ суб'єкта *S* до об'єкта *O* на активізацію процесу, записаного в *O* як дані (.exe). При цьому доступі формується деякий домен для перетворення, описаного в *O*, і передається керування відповідній програмі.

Служба захисту інформації може управляти траєкторіями процесів у системі зведенням до ***обмеження на доступ*** у кожний момент часу, тобто створюючи локальний вплив. Основна ж складність захисту інформації полягає в тому, що маючи можливість використовувати набір локальних обмежень на доступ у кожний момент часу, необхідно вирішувати глобальну проблему недопущення виходу будь-якої можливої в системі траєкторії процесів у несприятливий стан. Власне із цим пов'язане визнання, що об'єктно-суб'єктний підхід в наші часи дещо є застарілим.

Випробуваним сучасним методом боротьби зі складністю систем є **об'єктно-орієнтовний підхід**, який є основою сучасної технології програмування. Тому представляється природним прагнення поширити цей підхід і на системи кібербезпеки, для яких, як і для програмування в цілому, має місце згадана проблема складності.

Складність ця має двояку природу. По-перше, складними є не тільки апаратно-програмні засоби систем, які необхідно захищати, але й самі

засоби безпеки. По-друге, швидко зростає складність сімейства нормативних документів, які визначають вимоги до засобів безпеки.

Як вже вказувалось, вирішення проблем складності пов'язане з методологію декомпозиції. У даному контексті цей принцип означає, що складна система, у тому числі й система кібербезпеки, на верхньому рівні має складатися з невеликої кількості відносно незалежних, тобто з мінімальною кількістю зв'язків, компонентів. Потім декомпозиції піддаються виділені на першому етапі компоненти, і так далі до заданого рівня деталізації. У результаті система представляється у вигляді ієрархії з кількома рівнями абстракції.

Власне об'єктно-орієнтовний підхід й задовольняє таким вимогам. Нагадаємо, що об'єктно-орієнтовний підхід використовує *об'єктну декомпозицію*, тобто поведінка системи описується в термінах взаємодії об'єктів.

Розглядаючи об'єктно-орієнтовний підхід, окрім притаманних цьому методу певних визначень (клас, метод, об'єкт і т.ін.), слід увести два нових важливих поняття: *компонент і контейнер*.

Компонент – багаторазово використовуваний об'єкт, що допускає обробку й збереження в довгостроковій пам'яті.

Контейнери містять в собі множину компонентів, що створюють загальний контекст взаємодії з іншими компонентами й з оточенням.

Поняття компонента й контейнера важливі тому, що з їхньою допомогою ми можемо природно представити АС, що захищається, і самі захисні засоби. Наприклад, контейнер може визначати межі контрольованої зони (задавати так званий «периметр безпеки»).

Продемонструємо, як можна розглядати СППР, що захищається, варіюючи рівень деталізації використовуючи об'єктну декомпозицію.

Нехай деяка СППР розташована у двох зонах, у кожній з яких є сервери, що обслуговують внутрішніх і зовнішніх користувачів, а також користувачі, що потребують внутрішніх і зовнішніх сервісів. Одна з зон обладнана зовнішнім підключенням (тобто має вихід в Інтернет). При погляді з нульовим рівнем деталізації ми побачимо лише те, що на підприємстві є СППР, а саме:

СППР

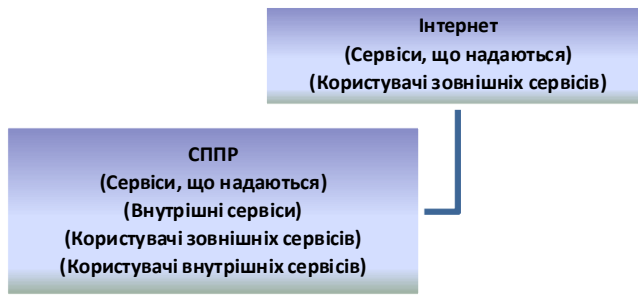
Подібне уявлення може показатися дуже загальним, але на цьому рівні вже можна врахувати, наприклад, необхідну нормативну базу,

можуть бути задекларовані цілі та основні завдання СППР, визначити вимоги до фізичної безпеки системи і шляхи їх виконання й т.ін.

Питання за якими критеріями проводити декомпозицію системи у значній мірі визначається особливостями конкретної СППР та підприємства, де вона використовується. Будемо вважати, що на першому рівні деталізації робляться видимими сервіси й користувачі, точніше, поділ на клієнтську й серверну частину:

На цьому рівні варто сформулювати вимоги до сервісів (до самої їхньої наявності, до доступності, цілісності й конфіденційності інформаційних послуг), викласти способи виконання цих вимог, визначити загальні правила поведінки користувачів, необхідний рівень їхньої попередньої підготовки, методи контролю їхньої поведінки, порядок заохочення й покарання й т.ін. Можуть бути сформульовані вимоги й переваги стосовно серверних і клієнтських платформ.

На другому рівні деталізації констатується тільки існування зв'язків з Інтернетом, наявність у них користувачів, а також зовнішніх і внутрішніх сервісів. Що це за сервіси, поки що не є важливим.



На рівні деталізації 2 також необхідно враховувати нормативну базу, зокрема щодо АС, які мають зовнішні підключення. Мова йде про допустимість такого підключення, про його захист, про відповідальність користувачів, що звертаються до зовнішніх сервісів, і про відповідальність організацій, що відкривають свої сервіси для зовнішнього доступу.

Треба звернути увагу на те, що контейнер «СППР» (у значенні компонентного об'єктного середовища) задає границі контрольованої зони, у межах яких підприємство проводить певну політику.

Таким чином, збільшуючи рівень деталізації можна розглянути дві окремі зони і канали зв'язку між ними, розподіл сервісів і користувачів по цих зонах і засоби забезпечення безпеки внутрішніх комунікацій, специфіку окремих сервісів, різні категорії користувачів і т.ін.

Прикладом застосування об'єктно-орієнтовного підходу до питань кібербезпеки є використання такого його поняття як *грані* – відносно незалежні характеристики об'єктів. Доступність, цілісність і конфіденційність фактично є трьома гранями кібербезпеки на верхньому рівні. Вважається, що якщо всі вони забезпечені, то забезпечена й безпека у цілому. Очевидно, що для виділених граней діє принцип інкапсуляції.

На завершення слід зазначити, що фахівці та науковці не обмежуються названими трьома підходами до розгляду проблем кібербезпека, продовжуючи пошук більш ефективних та універсальних підходів. Прикладом одного з таких є так званий системний підхід, який базується на дослідженнях, викладених у виданні «Безопасность информационных технологий. Системный подход» (автор В. В. Домарев). Враховуючи, що системність має місце й у вище розглянутих підходах, цей підхід доцільніше було б назвати «систематизованим», адже саме систематизація є сильною його стороною.

За задумом, систематизована модель повинна задовольняти трьом групам вимог, а саме вимогам *використання, властивостей та можливостей.*

Вимоги першої групи стосуються необхідності використання моделі в якості посібника зі створення СЗІ, методики формування показників і вимог до СЗІ, інструмента (методики) оцінки СЗІ, а також в якості моделі для проведення досліджень СЗІ.

Щодо властивостей модель повинна бути універсальною, комплексною, простою у використанні, наочною, практично спрямованою, самонавчальною (можливість нарощування знань) та функціональною в умовах високої невизначеності вихідної інформації.

Можливості моделі повинні дозволяти установлювати взаємозв'язок між показниками (вимогами), задавати різні рівні захисту, отримувати кількісні оцінки, контролювати стан СЗІ, застосовувати різні методики оцінок, оперативно реагувати на зміни умов функціонування, об'єднувати зусилля та досвід різних фахівців єдиним задумом.

Відповідаючи на питання як скласти таке уявлення про кібербезпеку, щоб охопити усі вимоги та аспекти проблеми, цей підхід базується на загальновизнаній думці, що людина отримує найбільш повне уявлення про явище, що його цікавить, коли йому вдається розглянути це щось невідоме з усіх боків, у тривимірному вимірі. Скориставшись цим принципом,

модель процесів кібербезпека розглядається у таких трьох «координатах» – трьох групах складових моделі (рис. 1.19): 1) із чого складається *(основи)*; 2) для чого призначена *(напрями)*; 3) як працює *(етапи)*.

Основами, як складовими частинами практично будь-якої складної системи (у тому числі й системи захисту інформації) є:

- законодавча, нормативно-правова й наукова база *(нормативи)*;
- структура й завдання органів *(підрозділів)*, що забезпечують безпеку *(органи)*;
- організаційно-технічні й режимні заходи й методи *(політика інформаційної безпеки)*;
- програмно-технічні способи й засоби *(засоби)*.

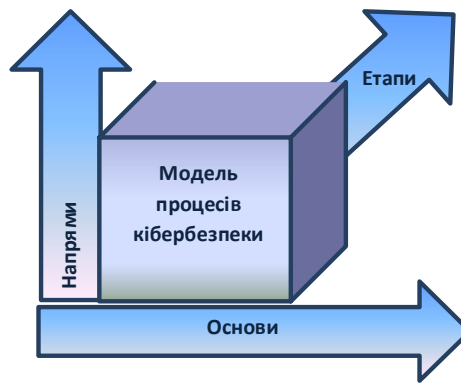


Рис. 1.19. Три «координати вимірів» систематизованої моделі кібербезпеки

Напрями формуються виходячи з конкретних особливостей АС як об'єкта захисту. У загальному випадку, з огляду на типову структуру АС і історично сформовані види робіт із захисту інформації, пропонуються наступні напрями:

- захист об'єктів автоматизованих систем *(об'єкти)*;
- захист процесів, процедур і програм обробки інформації *(процеси)*;
- захист каналів зв'язку та телекомунікацій *(канали)*;
- придушення побічних електромагнітних випромінювань *(ПЕМВН)*;
- керування системою захисту *(керування)*.

Оскільки кожен із напрямів базується на перерахованих вище основах, то елементи основ і напрямів мають розглядатися нерозривно один з одним. Наприклад, одну з основ за назвою *«нормативи»* необхідно розглядати в усіх напрямах, а саме:

1) законодавча база захисту *об'єктів*,
2) законодавча база захисту *процесів*,
3) законодавча база захисту *каналів*,
4) законодавча база *ПЕМВН*,
5) законодавча база по *керуванню*.

Аналогічно варто розглядати й інші грані основ в усіх напрямах.

Як бачиться, для формування загального подання про конкретну систему захисту необхідно відповісти мінімально на 20 (4х5=20) найпростіших питань.

Але це ще не все. Далі необхідно розглянути **етапи** (послідовність кроків) створення СЗІ, які необхідно реалізувати рівною мірою для кожного окремого напряму з урахуванням зазначених вище основ. Аналіз існуючих методик проведення робіт зі створення СЗІ дозволяє виділити наступні етапи:

- визначення інформаційних і технічних ресурсів, а також об'єктів АС, що підлягають захисту *(ресурси)*;
- виявлення повної множини потенційно можливих загроз і каналів витоку інформації *(загрози)*;
- проведення оцінки уразливості й ризиків інформації (ресурсів АС) при наявній множині загроз і каналів витоку *(ризики)*;
- здійснення вибору засобів захисту інформації і їхніх характеристик *(вибір)*;
- впровадження й організація використання обраних заходів, способів і засобів захисту *(впровадження)*;
- визначення вимог до системи захисту інформації *(вимоги)*;
- здійснення контролю цілісності й керування системою захисту *(контроль)*.

Оскільки етапів сім, і по кожному треба освітити 20 уже відомих нам питань, то в цілому для формування уявлення про конкретну систему захисту необхідно відповісти на 140 простих питань.

Все це можна представити у вигляді своєрідного кубика Рубіка, на гранях якого утворюється мозаїка взаємозалежних складових елементів моделі системи захисту.

Для простоти розуміння та наочності краще перетворити тривимірну фігуру у двомірну. Для цього тривимірний куб розгортається на площині (на аркуші паперу) і отримуємо перетворення тривимірної матриці у двомірну таблицю, що логічно об'єднує складові блоків «основи», «напрями» і «етапи» за принципом кожний з кожним. Звісно, що матриця у вигляді двомірної таблиці з'являється не сама по собі, а формується в кожно-

му конкретному випадку, виходячи з конкретних завдань щодо створення конкретної СЗІ для конкретної АС.

Елементи матриці повинні мати відповідну нумерацію. Наприклад, можна запропонувати таку систему трьохзначних позначень кожного з елементів матриці, коли перше знакомісце (X00) відповідає номерам складових блоку «етапи», друге (0X0) – номерам складових блоку «напрями», третє (00X) – номерам складових блоку «основи».

На рис. 1.20 наведено приклад формування елемента 321 матриці, що враховує наступні складові:

300 – проведення оцінки уразливості й ризиків (складова № 3 блоку «етапи»);

020 – захист процесів і програм (складова № 2 блоку «напрями»);

001 – нормативна база (складова № 1 блоку «основи»).

В табл. 1.4 наведено приклад змісту інформації для елементів матриці № 321, 322, 323, 324, які поєднують наступні складові:

№ 3 (300 проведення оцінки уразливості й ризиків) блоку «етапи»;

№ 2 (020 захист процесів і програм) блоку «напрями»;

№ 1, 2, 3, 4 (001 норматив, 002 органи, 003 політика, 004 заходи) блоку «основи».

Це зміст тільки чотирьох питань зі ста сорока, але відповіді на них уже дозволяють сформувати якесь уявлення про стан справ по захисту інформації в конкретній АС. Опис же усіх 140 питань дозволяє скласти повне уявлення про СЗІ й оцінити досягнутий рівень захисту.

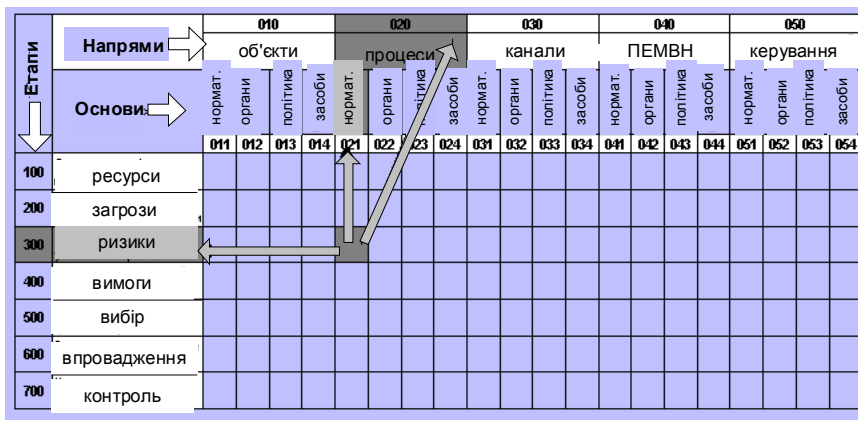


Рис. 1.20. Приклад формування елемента №321 матриці моделі СЗІ у вигляді таблиці

Таблиця 1.4

Зміст інформації для елементів матриці № 321, 322, 323, 324

№ елементу	Зміст інформації в елементі
321	Наскільки повно відображені в законодавчих, нормативних і методичних документах питання, що визначають порядок проведення оцінки уразливості й ризиків для інформації, що використовується в процесах і програмах АС
322	Чи є структура органів (співробітники, керівники), відповідальна за проведення оцінки уразливості й ризиків для процесів і програм АС
323	Чи визначені режимні заходи, що забезпечують своєчасне і якісне проведення оцінки уразливості й ризиків для інформації використовуваної в процесах і програмах АС
324	Чи застосовуються технічні, програмні або інші засоби для забезпечення оперативності і якості проведення оцінки уразливості й ризиків у процесах і програмах АС

В принципі зробити це достатньо складно. Однак саме такий підхід дає можливість тримати правильний напрямок у процесі створення складних систем захисту. Оскільки при цьому постійно враховуються взаємні логічні зв'язки між численними елементами СЗІ, є шанс побудувати саме систему, а не набір окремих рішень. Нагадаємо, запорукою є те, що матриця формується виходячи з опису конкретної АС і конкретних завдань щодо захисту інформації в цій системі.

Таким чином, запропонована модель подання СЗІ у вигляді тривимірної матриці дозволяє не лише жорстко відслідковувати взаємні зв'язки між елементами системи захисту, але може виступати й в ролі посібника зі створення СЗІ. Якщо, приступаючи до створення системи захисту, спробувати відповісти на пропоновані загальні питання, стане зрозумілим що вже є, а чого не вистачає для досягнення поставленої мети. Фактично, заповнивши 140 елементів матриці відповідними вимогами, можна одержати досить повне технічне завдання на створення СЗІ. Слід додати до цього, що сформулювати ці вимоги можна на основі будь-яких стандартів – міжнародних, європейських, українських, в залежності від того, які узяти нормативи у блоку «основи».

Підхід на основі тривимірної матриці дозволяє також оцінити ефективність створюваної або вже функціонуючої СЗІ. Тільки тепер по 140 показниках (елементах матриці) треба виставити відповідні оцінки. Існує чимало методів оцінок, треба лише вибрати такий, що буде зрозумілим і прозорим у конкретній організації. Опрацювання такої об'ємної матриці можливе лише за допомогою комп'ютера. Існують відповідні програми, зокрема для оцінки ефективності СЗІ.

Можливість оцінки ефективності СЗІ на основі підходу систематизації та тривимірної матриці, яка була розглянутою, демонструє ще одну з переваг такого підходу до створення систем захисту інформації.

1.3.3. Основні моделі кібербезпеки

Основним методом аналізу систем забезпечення кібербезпеки, як і взагалі для складних систем, є створення відповідних моделей. Основне призначення таких моделей в сфері безпеки полягає в створенні передумов для об'єктивної оцінки загального стану АС з точки зору міри уразливості або рівня захищеності інформації в ній. Необхідність в таких оцінках зазвичай виникає при проведенні аналізу з метою вироблення рішень щодо організації захисту інформації.

Теоретичні основи побудови формальних моделей систем забезпечення кібербезпеки є надзвичайно складними, і незважаючи на інтенсивні дослідження у цій сфері, що проводяться, вони ще далекі від успіху. Тому практичного застосування отримали неформальні (описові) моделі, такі як загальна модель захисту інформації, модель загроз інформації, модель порушника, модель аналізу систем розмежування доступу до ресурсів АС, тощо.

Ці моделі в найзагальнішому вигляді відображають процес захисту інформації як процес взаємодії дестабілізуючих чинників, що впливають на інформацію, і засобів захисту інформації, що перешкоджають дії цих чинників. Підсумком такого моделювання має бути визначення того або іншого рівня захищеності інформації. Також вказані процеси в найзагальнішому вигляді можуть бути представлені як процеси розподілу і використання ресурсів, що виділяються на захист інформації. Основною спрямованістю є оцінка не просто загроз інформації як таких, а ще й оцінка тих втрат, які можуть мати місце при проявах різних загроз. Моделі цього напряму важливі ще і тим, що саме на них найбільшою мірою виявляються ті умови, при яких забезпечується вирішення завдань аналізу і синтезу систем (механізмів) розмежування доступу до різних видів ресурсів АС. Важливість цих моделей обумовлена й тим, що механізми розмежування доступу належать до найбільш суттєвих компонентів систем захисту інформації, від ефективності функціонування яких, значною мірою, залежить ефективність забезпечення кібербезпека в цілому.

Серед напрацьованих моделей безпеки, які можливо представити у формалізованому виді, передусім необхідно виділити моделі політики безпеки. Як визначено у Критеріях захищеності комп'ютерних систем (TCSEC), політика безпеки – це набір норм, правил і практичних прийомів, які регулюють керування цінною інформацію, її захист і розподіл. Таке

визначення політики безпеки дає змогу застосувати формалізований апарат для її опису. Поняття політики пов'язане із поняттям доступів, при чому як дозволених, так і недозволених.

Враховуючі фундаментальність «Оранжевої книги», її загальновизнаний понятійний базис, без якого навіть обговорення проблем кібербезпеки важко уявити, необхідно особливо звернути увагу на уведені цим документом поняття *політики безпеки, механізмів безпеки і класів безпеки*.

Політика безпеки повинна обов'язково містити в собі деякі з наступних елементів механізмів безпеки:

- довірче керування доступом;
- примусове (адміністративне) керування доступом;
- мітки безпеки;
- безпека повторного використання об'єктів.

Довірче керування доступом *(називане іноді дискреційним)* – це метод розмежування доступу до об'єктів, заснований на обліку особистості суб'єкта або групи, у яку суб'єкт входить. Довільність керування полягає у тому, що деяка особа (звичайно власник об'єкта) може за своїм розсудом надавати іншим суб'єктам права доступу до об'єкта або відбирати їх в них.

Спосіб керування доступом називається примусовим, оскільки він не залежить від волі суб'єктів (навіть системних адміністраторів). Іноді його називають *мандатним*.

Для реалізації примусового керування доступом із суб'єктами й об'єктами асоціюються *мітки безпеки.* Мітка суб'єкта описує його благонадійність, мітка об'єкта – ступінь конфіденційності інформації, що утримується в ньому. Суб'єкт може читати інформацію з об'єкта, якщо рівень таємності суб'єкта не нижче, ніж в об'єкта, а всі категорії, перераховані в мітці безпеки об'єкта, присутні в мітці суб'єкта. Зміст сформульованого правила зрозумілий – читати можна тільки те, що дозволено. Також суб'єкт може записувати інформацію в об'єкт, якщо мітка безпеки об'єкта домінує над міткою суб'єкта. Зокрема, «конфіденційний» суб'єкт може записувати дані в секретні файли, але не може – у несекретні (зрозуміло, повинні також виконуватися обмеження на набір категорій).

Важливим доповненням засобів керування доступом, що охороняє від випадкового або навмисного добування конфіденційної інформації зі «сміття», є *безпека повторного використання* об'єктів. Вона повинна гарантуватися для областей оперативної пам'яті (зокрема, для буферів з образами екрана, розшифрованими паролями й т.п.), для дискових блоків і магнітних носіїв у цілому.

Виходячи з цього у сучасній теорії захисту інформації розглядають такі політики безпеки: дискреційна, або розмежування доступу *(DAC – Discretionary Access Control)*, мандатна, або багаторівнева *(MAC – Mandatory Access Control)*, ролевого розмежування доступів *(RBAC – Role Based Access Control)*, ізольованого програмного середовища, безпеки інформаційних потоків. Можливі й інші політики безпеки, у тому числі комбіновані з названих.

Формальна модель політики безпеки *(Formal security policy model)* – модель політики безпеки, виражена точним, можливо математичним способом, що включає початковий стан системи, способи переходу системи з одного стану в інший й визначення безпечного стану системи.

Основою *дискреційної* політики безпеки є виборче керування доступом, яке передбачає, що:

- усі суб'єкти й об'єкти системи повинні бути ідентифіковані;
- права доступу суб'єкта до об'єкта системи визначаються на підставі деякого правила (властивість вибірковості).

Основним елементом дискреційної політики безпеки є матриця доступу – матриця D розміром $|S|x|O|$. Кожний елемент цієї матриці визначає права доступу з множини прав R суб'єкта s до об'єкта o (рис. 1.21).

Рис. 1.21. Матриця доступу дискреційної політики безпеки

Підмножина об'єктів, до яких суб'єкт має визначені права доступу, має назву домену цього суб'єкту.

Матриця доступу як правило є дуже розрідженою. Замість матриці на практиці застосовують списки доступу (асоціюють з об'єктом) та списки повноважень (асоціюють з суб'єктом).

До переваг дискреційної політики необхідно віднести легкість її реалізації на практиці. Серед недоліків виділяються її статичність, яка не враховує

динаміку змін у системі, алгоритмічна нерозв'язуваність задачі перевірки безпеки, а також нечутливість до «троянських коней». Практична діяльність в сфері безпеки довела, що дискреційна політика найкращим чином пристосована для вирішення проблем контролю доступу в АС цивільного призначення.

Поміж моделей аналізу систем захисту, що реалізують дискреційну політику, дві найвідоміші – це модель Харрісона – Руззо – Ульмана (модель ХРУ) і модель Take-Grant.

У моделі ХРУ розглядається модифікація матриці доступу із використанням низки примітивних операторів. З цих операторів складають команди, якими описують переходи системи зі стану в стан.

Модель Take-Grant допускає наявність прав доступу не лише у суб'єктів до об'єктів, але й в об'єктів до об'єктів. Ця модель призначена для аналізу шляхів розповсюдження прав доступу за вихідним графом прав доступу в системах дискреційного розмежування доступу.

Мандатна *(повноважна, нормативна, примусова)* політика безпеки передбачає виконання таких умов:

- визначеність решітки конфіденційності інформації;
- надання кожному об'єкту системи певного рівня конфіденційності (цінності);
- усі суб'єкти й об'єкти системи повинні бути ідентифіковані.

Головне завдання мандатної політики безпеки полягає у запобіганні витоку інформації від об'єктів, що мають високий рівень доступу, до об'єктів із низьким рівнем доступу. Мандатна ПБ спрямована на захист інформації в АС організацій, що працюють з критичною інформацією, де є необхідним багаторівневе розмежування повноважень і прав доступу згідно з допусками до обробки інформації тієї чи іншої категорії.

Мандатна політика має низку переваг, а саме:

- правила мандатної політики є більш прозорими та зрозумілими порівняно з дискреційною політикою безпеки;
- системи з мандатною політикою більш надійні;
- задача перевірки безпеки є алгоритмічно розв'язуваною.

До недоліків необхідно віднести складність у реалізації, і як наслідок високі вимоги до обчислювальних ресурсів, що її підтримують.

Дві найпоширеніші моделі аналізу систем захисту, які реалізують мандатну політику – це модель мандатної політики конфіденційності Белла – ЛаПадула та модель мандатної політики цілісності Біба, яка базується на моделі Белла – Лападула.

Модель Белла – ЛаПадула є базовою моделлю мандатної політики безпеки. Зазвичай цю модель застосовують для аналізу систем захисту

інформації на імовірність наявності умов виникнення інформаційних потоків від об'єктів, що мають більший рівень конфіденційності, до об'єктів із меншим рівнем конфіденційності. Будь-який суб'єкт (крім адміністратора безпеки, якому надано повноваження встановлювати рівні конфіденційності об'єктів) жодним чином не зможе здійснити перенесення даних із об'єкта з вищим рівнем конфіденційності в об'єкт, що має нижчий рівень конфіденційності (рис. 1.22).

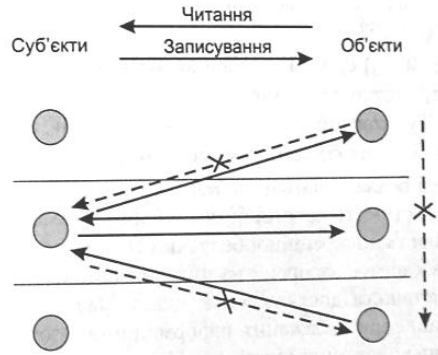


Рис. 1.22. Можливості перенесення даних за моделлю Белла – ЛаПадула мандатної політики безпеки

На відміну від моделі конфіденційності Белла – ЛаПадула, модель безпеки Біба застосовують для забезпечення мандатної політики цілісності. Найвагомішу загрозу цілісності інформації (імовірність модифікації або знищення) може становити записування інформації вверх суб'єктом із нижчого рівня безпеки інформації. Інколи читання інформації суб'єктом із низьким рівнем безпеки з об'єкта, що має більш високий рівень, також може нести загрозу її цілісності. Для уникнення цих загроз цілісності природно використовувати заборону записування інформації вверх, а також заборону читання інформації знизу. Методологічною основою моделі Біба с модель Белла – ЛаПадула за умови, що правила моделі Біба є інверсією правил моделі Белла – ЛаПадула.

Також необхідно відмітити важливість ролевої політики, яка базується на дискреційній політиці і є її розвитком. У цій політиці права доступу суб'єктів формуються на підставі їх ролей, які пов'язані з їх повноваженнями та обов'язками. Ця політика відрізняються гнучкістю і її використовують там, де чітко розподілені права адміністраторів і користувачів (доступ до БД, мережні ОС та ін.).

Звичайно, при виборі політики безпеки необхідно враховувати види доступів до інформації, особливості її обробки, організаційну структуру АІС, сферу її застосування, можливі канали витоку інформації та багато інших важливих факторів. Тим не менш, рольова політика дозволяє більш гнучко, ніж інші види політик регламентувати доступ до інформації. Наявність рис дискреційної та мандатної політик дозволяє впроваджувати її в більшості типів АІС, зокрема і в системах підтримки прийняття рішень.

Незважаючи на те, що рольова політика має багато переваг в порівнянні з іншими в питаннях управління безпекою, основна з яких є гнучкість у використанні, розробка її формалізованої, несуперечливої та уніфікованої моделі триває. Тим не менш, американським Національним Інститутом стандартів і технологій (NIST) вже створено стандарт з рольової ПБ, який передбачає певну модель цієї політики.

Згідно з вказаним стандартом модель рольової політики містить в собі чотири компонента:

- ядро;
- модель ієрархії ролей;
- модель бази даних авторизацій;
- модель активації.

Ядро є необхідним компонентом при розробці рольової політики, позаяк інші є незалежними і можуть бути імплементовані окремо. Зв'язок компонентів рольової політики показано на рис. 1.23.

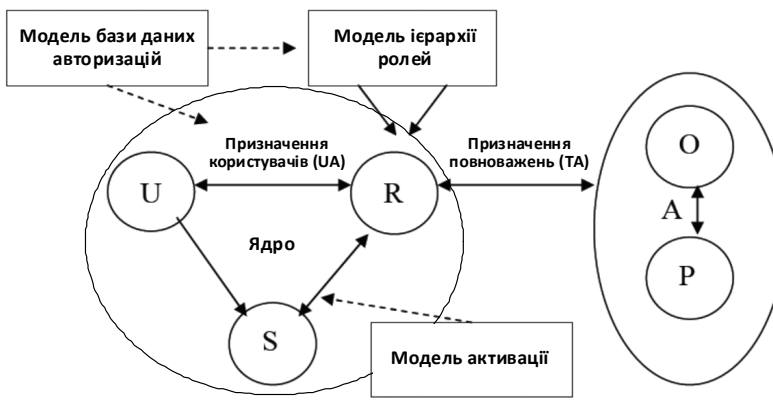


Рис. 1.23. Зв'язок компонентів моделі рольової політики

Ядро рольової політики фактично реалізує розмежування доступу *A* і містить набори основних типів і відношень між ними. Базовими відно-

шеннями є «користувач-роль» та «роль-повноваження», які полегшують розподіл повноважень між користувачами *U*.

Суть даної політики полягає в тому, що не користувач або процес (*P*) асоційовані з об'єктами (*O*), як це спостерігалось в дискреційній та мандатній політик, а роль (*R*) асоційована з набором повноважень. Отже, користувач може отримати певний доступ упродовж сеансу *S* роботи в системі до об'єкта тільки тоді, коли він є членом ролі, якій призначено відповідні повноваження.

Слабким місцем ролевої політики є надзвичайні повноваження адміністратора безпеки, який «нарізає» ролі користувачам, що може збільшити імовірність реалізації внутрішніх загроз, пов'язаних із людським фактором.

1.3.4. Класи безпеки

Важливим здобутком «Оранжевої книги» є створення базису для ранжування автоматизованих інформаційних систем по ступені довіри безпеки.

В документі визначається чотири рівні довіри – D, C, B і A. Рівень D призначений для систем, визнаних незадовільними. У міру переходу від рівня C до A до систем пред'являються усе більш жорсткі вимоги. Рівні C і B підрозділяються на класи (C1, C2, B1, B2, B3) з поступовим зростанням ступеня довіри.

Класифікацію, уведену в «Оранжевій книзі», коротко можна сформулювати так:

рівень C – довірче керування доступом;

рівень B – примусове керування доступом;

рівень A – верифікуєма безпека.

Отже, усього є шість класів безпеки – C1, C2, B1, B2, B3, A1. Щоб у результаті процедури сертифікації систему можна було віднести до деякого класу, її політика безпеки й рівень гарантованості повинні задовольняти заданим вимогам, з яких ми згадаємо лише найважливіші.

Клас C1. Захист, заснований на розмежуванні доступу (DAC). Довірча, або гарантовано захищаюча обчислювальна база *(TCB – Trusted Computing Base)* систем класу (C1) забезпечує розділення користувачів і даних. Вона включає засоби керування, здатні реалізувати обмеження по доступу, щоб захистити приватну інформацію й не дати іншим користувачам випадково зчитувати або руйнувати дані. Передбачається, що середовище класу (C1) є таким, у якому можуть кооперуватися користувачі, що обробляють дані, приналежні одному й тому ж рівню таємності.

Клас C2. Захист, заснований на керованому контролі доступом. Всі вимоги до класу (C1) переносяться на клас (C2). Крім того, системи цього

класу реалізують структурно більш «тонке» керування доступом за рахунок додаткових засобів керування розмежуванням доступу й поширенням прав, а також за рахунок системи реєстрації подій (аудит), що мають відношення до безпеки системи й розподілу ресурсів. Спеціально вводиться вимога по «очищенню» ресурсів системи при повторному використанні іншими процесами.

Клас B1. Мандатний захист. Заснований на присвоюванні міток об'єктам і суб'єктам, що перебувають під контролем ТСВ. Вимоги для систем класу (B1) передбачають виконання всіх вимог, які були необхідні в класі (C2). Крім цього, необхідно представити неформальне визначення моделі, на якій будується політика безпеки, присвоювання міток даним і мандатне керування доступом пойменованих суб'єктів до об'єктів. У системі необхідно мати засіб, що дозволяє точно й надійно присвоювати мітки експортованої інформації.

Клас B2. Структурований захист. Всі вимоги класу (B1) повинні виконуватися для системи класу (B2). У системах класу (B2) ТСВ заснована на чітко визначеній і формально задокументованій моделі, у якій керування доступом поширюється тепер на всі суб'єкти й об'єкти даної АС. Крім цього, повинен бути проведений аналіз, пов'язаний з наявністю побічних каналів витоків. Необхідно провести розбивку структури ТСВ по елементах, критичних з погляду захисту, і некритичних, відповідно. Інтерфейс ТСВ добре визначений, а проект і реалізація ТСВ виконані так, що вони дозволяють проводити ретельне тестування й повний аналіз. Механізми автентифікації посилені, керування захистом передбачається у вигляді засобів, призначених для адміністратора системи й для оператора, а на керування конфігурацією накладаються жорсткі обмеження. Система відносно стійка до спроб проникнення в неї.

Клас B3. Всі вимоги для систем класу (B2) включені у вимоги до систем класу (B3). Крім того, ТСВ класу (B3) повинна реалізовувати концепцію так званого монітора звернень (RM), який обробляє всі звернення у системі і є гарантовано захищеним від несанкціонованих змін, псування й підробки. Передбачається введення адміністратора безпеки системи, механізми контролю (аудит) розширені так, щоб забезпечити обов'язкову сигналізацію про всі події, пов'язані з можливим порушенням установлених у системі правил безпеки.

Клас AI. Системи цього класу функціонально еквівалентні системам класу (B3) у тому відношенні, що в них не з'являються які-небудь нові вимоги до політики забезпечення безпеки. Відмітною рисою систем даного класу є аналіз ТСВ, заснований на формальній специфікації проекту й

верифікації ТСВ, і, у підсумку, високий ступінь упевненості в тому, що гарантовано захищаюча обчислювальна база реалізована правильно. Такого роду гарантія починається вже з формальної моделі політики забезпечення безпеки і формальної специфікації проекту високого рівня.

1.3.5. Функціональні профілі захищеності

Нормативні документи Держспецзв'язку, зокрема НД ТЗІ 1.1.-002-99, НД ТЗІ 2.5.-005-99 вводять *функціональні профілі* захищеності, що є переліком мінімально необхідних рівнів послуг, які повинен реалізовувати КЗЗ комп'ютерної системи, щоб задовольняти певні вимоги до захищеності оброблюваної інформації. *Стандартні функціональні профілі* формуються на основі існуючих вимог до захисту певної інформації від певних загроз і відомих на сьогодні функціональних послуг, що дозволяють протистояти загрозам і забезпечити виконання цих вимог.

Опис профілю складається з трьох частин:

1) літерно-числового ідентифікатора;

2) знака рівності;

3) переліку рівнів послуг у фігурних дужках.

Ідентифікатор у свою чергу включає:

- позначення класу АС (1, 2 або 3);
- літерну частину, що характеризує види загроз, від яких забезпечується захист (К- конфіденційність, і/або Ц – цілісність, і/або Д – доступність);
- номер профілю;
- необов'язкове літерне позначення версії.

Усі частини ідентифікатора відокремлюються одна від одної крапкою.

Наприклад, 2.К.4 – функціональний профіль номер чотири, що відображає вимоги до АС класу 2, основна вимога щодо захисту оброблюваної інформації – забезпечення конфіденційності.

Низка нормативних документів Держспецзв'язку визначають вимоги до профілів захищеності КЗЗ, що входять до складу АС різних класів і призначень (наприклад, АС, які призначені для автоматизації банківської діяльності або органів державної влади).

Контрольні запитання та завдання

1. Для чого потрібна теорія захисту інформації?
2. Дайте визначення політики безпеки і критерію безпеки.

3. У чому полягає відмінність формального і неформального підходів в теорії захисту інформації?

4. Які напрацьовано підходи до забезпечення кібербезпеки як методологічної бази розгляду її проблем?

5. Сутність процесного підходу до забезпечення кібербезпеки, переваги та недоліки.

6. Особливості підходу «об'єкти-суб'єкти".

7. Переваги об'єктно-орієнтовного підходу.

8. На чому оснований систематизований підхід?

9. Поясніть сутність визначення класів безпеки АС.

10. Що таке функціональний профіль захищеності?

2. ОСНОВНІ ЗАХОДИ З ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ СППР

2.1. ОСНОВНІ ОРГАНІЗАЦІЙНО-ТЕХНІЧНІ ЗАХОДИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ СППР

Особливості сучасних автоматизованих систем, істотні з погляду безпеки.
Класифікація засобів забезпечення інформаційної безпеки.
Організаційне забезпечення.
Служби безпеки.

2.1.1. Особливості побудови сучасних СППР, істотні з погляду безпеки

Для СППР, за допомогою яких приймаються часто-густо дуже важливі і відповідальні рішення, питання створення захищеної системи є вельми важливими. Це питання ускладнюється у зв'язку із тим, що зміст проблем, пов'язаних з кібербезпекою, для різних типів систем та підприємств, де вони застосовуються, може істотно розходитися, адже на цей час сформувалося чимало типів СППР, що відрізняються за різними ознаками – за кількістю користувачів, за технічними характеристиками, в залежності від типів даних, з якими ці системи працюють та ін. Загальноприйнятий поділ СППР на концептуальному рівні наведено на рис. 2.1.

У зв'язку із цим до основних архітектурних принципів кібербезпеки СППР слід віднести:

- безперервність захисту в просторі й часі, неможливість оминути захисні засоби;
- слідування визнаним стандартам, використання апробованих рішень;
- ієрархічна організація СППР із невеликою кількістю сутностей (складових) на кожному рівні;

- особливе посилення найслабкішої ланки;
- неможливість переходу системи в небезпечний стан;
- мінімізація привілеїв користувачів та чіткий розподіл їх обов'язків;
- ешелонування оборони та розмаїтість захисних засобів;
- мінімізація обсягу захисних засобів, що виносяться на клієнтський рівень системи;
- простота побудови та керованість СППР.

Рис. 2.1. Концептуальна класифікація систем підтримки прийняття рішень

Виходячи з цих принципів, загальну структуру захищеної СППР можна представити на рис. 2.2. Безпека в ній підтримується політикою безпеки та комплексом засобів захисту (КЗЗ).

Але досвід свідчить, що в сучасних умовах одних технічних і програмних засобів є недостатніми для забезпечення належного рівня безпеки системи. Наявність людського фактору, несприятливого зовнішнього середовища вимагає вжиття додаткових засобів і заходів, передусім організаційного характеру, які спрямовані перш за все на людину. За деякими даними, до них відносяться більш ніж половина з усіх заходів з захисту інформації, що на цей час застосовуються. До цієї групи заходів відносяться й заходи, пов'язані із нормативно-правовим забезпечення безпеки та підтримкою морально-етичних норм.

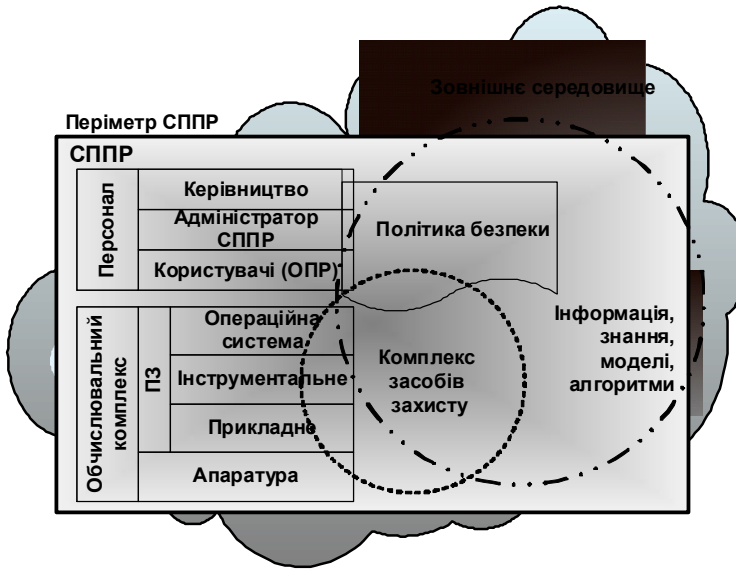


Рис. 2.2. Загальна структура захищеної СППР

Водночас, відповідно до визначення кібербезпеки, вона залежить не тільки від комп'ютерів і мереж комунікацій, від персоналу, що обслуговує, але й від підтримуючої інфраструктури, до якої можна віднести системи охорони приміщень, електро-, водо- і теплопостачання, кондиціонери, тощо. Ця інфраструктура має самостійну цінність, але, водночас, вона впливає й на забезпечення кібербезпеки при виконанні передбачених автоматизованою системою функцій.

Таким чином, способи впливу дестабілізуючих факторів або причини, що їх породжують, на систему, на її елементи, на інформацію, на моделі та алгоритми, з одного боку, а з іншого – урахування прагнення підвищення значень показників захищеності визначають множину і розмаїтість можливих видів захисту СППР. Відповідно способи, засоби і заходи забезпечення безпеки СППР можуть бути класифіковані наступним чином (рис. 2.3).

Засоби і заходи поділяються на формальні і неформальні. До формальних відносяться апаратні та програмні засоби, а також так звані фізичні.

Апаратні засоби – це різні електронні, електронно-механічні і подібні пристрої, що вбудовуються в апаратуру обчислювального комплексу СППР або сполучаються з нею спеціально для розв'язання задач захисту інформації.

Програмні засоби – спеціальні пакети програм чи окремі програми, що використовуються для вирішення завдань захисту.

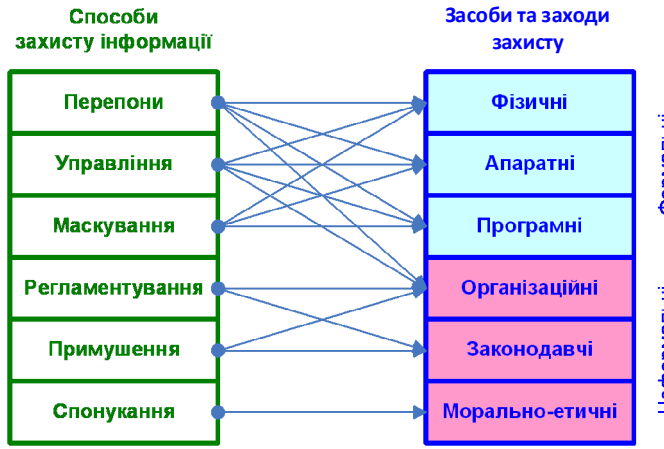


Рис. 2.3. Способи, засоби і заходи забезпечення безпеки СППР

Фізичні засоби – механічні, електричні, електромеханічні, електронні, електронно-механічні й інші пристрої і системи, що функціонують автономно, створюючи різного роду перешкоди дестабілізуючим факторам.

До неформальних відносяться організаційні заходи, законодавчі, а також заходи забезпечення морально-етичних норм.

Організаційні заході – заходи, що передбачаються спеціально з метою вирішення задач захисту організаційними мірами.

Правові заході – державні законодавчо-правові акти, пов'язані з забезпеченням захисту інформації, які регламентують права й обов'язки всіх осіб і підрозділів, що мають відношення до підтримки функціонування та використання СППР, і встановлюють відповідальність за дії, наслідком яких може бути порушення захищеності інформації.

Морально-етичні норми – це сформовані в колективі моральні норми й етичні правила, дотримання яких сприяє захисту інформації, а порушення їх прирівнюється до недотримання правил поведінки на підприємстві.

З вказаними засобами і заходами пов'язаний комплекс способів захисту, які можуть вживатися в оточенні системи.

Найважливіше значення мають управлінські способи, за допомогою яких регулюється використання усіх ресурсів системи (технічних, програмних, інформаційних, людських), зокрема забезпечується управління

доступом. До управлінських способів примикають способи регламентування, які забезпечують порядок інформаційної діяльності з урахуванням норм і вимог безпеки для всіх періодів життєвого циклу об'єкта захисту. Маскування як здатність ставати невидимим в очах ворога є поширеним способом захисту інформації, зокрема з використанням інженерних, технічних засобів, а також шляхом криптографічного закриття інформації. Наприклад, для забезпечення захищеності інформації від витоку через побічні електромагнітні випромінювання у електронних засобах маскування полягає у використанні активного радіотехнічного обладнання та методів екранування об'єктів. Нарешті, способи примушення і спонукання, які вживаються, як правило, керівництвом підприємства та уповноваженими особами за підтримки нормативного забезпечення спрямовані на персонал, який має відношення до користування системою та її обслуговування, з метою звести до мінімуму спроби людей втрутитися у нормальний процес функціонування системі шляхом роз'яснювальної роботи, навчання та відповідного інформування. Як відомо, значну кількість людей втримує від протиправних дій усвідомлення того, що це засуджується й/або карається суспільством, або тому, що так робити не прийнято.

Виходячи з цього увесь комплекс забезпечення кібербезпеки СППР вбачається як складне утворення. Перевіреним способом подолання таких складностей є структурування за рівнями представлення. На рис. 2.4 наведено основні рівні забезпечення кібербезпеки СППР.

Рис. 2.4. Основні рівні забезпечення кібербезпеки СППР

До *адміністративного рівня* кібербезпеки відносяться дії загального характеру, що вживаються керівництвом підприємства. Законодавчий рівень, що утворює нормативно-методичну базу безпеки, вважається найважливішим серед інших рівнів, адже він створює умови для скоординованого розвитку засобів захисту та сприяє запобіганню «самодіяльності» у цій сфері.

Організаційний рівень складають заходи, що передбачаються спеціально з метою вирішення задач захисту організаційними мірами. До таких заходів відноситься, зокрема, утворення на підприємстві, де експлуатується СППР, спеціальної *служби інформаційної безпеки*. Як вказувалося, безпека СППР залежить від оточення, у якому вона функціонує. Тому необхідним є вжиття заходів для захисту будинків і прилеглої території, підтримуючої інфраструктури, обчислювальної техніки, носіїв даних. Такі заходи відносяться до *інженерно-технічного рівня* (іноді їх ще називають *фізичними*).

Нарешті, технічною (комп'ютерною) основою захисту СППР є програмно-технічний рівень, що передбачає застосування програмних і апаратних засобів, які формують *систему захисту інформації* (СЗІ), яка є невід'ємною частиною програмно-апаратних засобів СППР, її самостійною підсистемою.

СЗІ є сукупністю спеціальних програмно-апаратних засобів, інтегрованих в СППР, а також спеціалізованих автоматизованих робочих місць (АРМ), що входять до складу СППР, для керування СЗІ та моніторингу безпеки.

Головною властивістю СЗІ повинна бути її здатність до пристосування при зміні технологічних схем чи умов функціонування СППР. Додатковими принципами можуть бути:

- мінімізація витрат при максимальному використанні серійних засобів;
- забезпечення вирішення необхідної сукупності задач захисту;
- комплексне використання засобів захисту, оптимізація архітектури;
- зручність для персоналу;
- простота експлуатації та адміністрування.

Як свідчить досвід та приписують нормативні документи, ефективно вирішувати завдання щодо захисту інформації, що циркулює в АІС, а також забезпечити надійний захист АІС від злочинних посягань (у тому числі й з-за меж країни) можливо лише шляхом створення *в їх складі комплексних систем захисту інформації* (КСЗІ), що поєднують правові, організаційні, інженерні заходи, а також технічні і програмні засоби захисту.

2.1.2. Організаційне забезпечення та служба інформаційної безпеки СППР

Організаційні заходи полягають у наступному:

- визначення технологічних процесів з прийняття рішень, що підтримуються системою;
- вибір завдань захисту;
- розробка правил забезпечення безпеки;
- визначення обов'язків посадових осіб та користувачів;
- вибір засобів захисту;
- створення нормативних документів;
- визначення зон кібербезпеки;
- обґрунтування структури СЗІ;
- встановлення порядку впровадження СЗІ;
- атестація СЗІ.

Організаційне забезпечення охоплює усі стадії створення СППР та СЗІ – проектування, розробка, виготовлення, впровадження, підготовка до експлуатації, експлуатація, виведення з експлуатації.

Для виконання організаційних заходів створюються спеціальні структурні органи (підрозділи). Під поняттям «структурні органи» мається на *увазі служба інформаційної безпеки* (СІБ). В залежності від масштабів СППР, СІБ може бути представленою від одного до кількох працівників. Відповідно склад, призначення і функції СІБ можуть значною мірою варіюватись. Заздалегідь відзначимо, що структура СІБ повинна:

- керуватися нормативною базою, де описані її склад, призначення і функції;
- діяти відповідно до встановлених заходів, тобто виконувати прийняту на підприємстві політику безпеки;
- мати у своєму розпорядженні відповідні засоби, іншими словами – технічне та програмне оснащення.

Стосовно нормативної бази слід зазначити, що основним документом є політика безпеки, положення якої повинні бути закріплені у відповідних розпорядницьких документах, склад і зміст яких визначаються специфікою СППР. Однак, як правило, жодна система не зможе обійтися без додаткової низки документів, які визначають положення про комерційну (державну) таємницю, про захист інформації, про адміністратора безпеки мережі, про розмежування прав доступу до інформації, що міститься в системі, а також правил допуску в приміщення, де здійснюється обробка критичної інформації та порядку проведення службового розслідування по фактах порушення правил безпеки.

Серед нормативних документів чинне місце має займати перелік обов'язкових заходів, спрямованих на вироблення плану та забезпечення дій з захисту СППР самої СІБ, а саме: визначення складу СІБ, її місце в організаційній структурі підприємства, сфера її компетенції, права і повноваження, варіанти дій у різних ситуаціях для запобігання конфліктів між підрозділами.

Роботи з оснащення і підтримки діяльності СІБ, створення системи розпорядницьких документів входять у комплекс організаційних заходів, на основі якого може бути досягнуто високий рівень безпеки. Проте, перераховані заходи не дозволять на належному рівні підтримувати функціонування системи захисту без цілого ряду організаційно-технічних заходів. Їхній повний перелік занадто широкий для того, щоб цілком приводити його в цьому курсі. Вкажемо лише, що їх проведення дозволяє вчасно виявляти нові канали витоку інформації, вживати заходів з їх нейтралізації, удосконалення системи захисту, оперативно реагувати на порушення режиму безпеки. При цьому необхідно враховувати, що гарантувати безпеку СППР та виявлення уразливих місць може лише використання якісних комерційних технічних інструментів безпеки, оскільки у комерційних системах засоби захисту оновлюються досить оперативно.

Стосовно задач, які розв'язують служби інформаційної безпеки СППР, необхідно зазначити, що основною задачею СІБ є визначення напрямку розвитку і підтримки зусиль, націлених на захист інформації в СППР від несанкціонованого ознайомлення, зміни, руйнування, відмовлення в доступі. Це досягається шляхом упровадження відповідних правил, інструкцій і вказівок. Тому СІБ відповідає за розробку і виконання планів щодо забезпечення безпеки, що стосуються наступних основних напрямків:

- розробка і видання правил (інструкцій і вказівок) щодо забезпечення безпеки СППР, які відповідають загальним правилам роботи підприємства і вимогам до обробки інформації;
- упровадження програми забезпечення безпеки, включаючи класифікацію ступеня конфіденційності або таємності інформації (якщо така є) і оцінку діяльності;
- розробка і забезпечення виконання програми навчання й ознайомлення з основами інформаційної безпеки СППР;
- розробка і супровід переліку мінімальних вимог до процедур контролю за доступом до СППР;
- добір, упровадження, перевірка й експлуатація відповідних методик планування відновлення роботи для всіх підрозділів організації, що приймають участь в обробці найважливішої інформації в СППР;

- розробка і впровадження процедур перегляду правил забезпечення інформаційної безпеки, а також робочих програм, призначених для підтримки правил, інструкцій, стандартів і вказівок;
- участь у вивченні, оцінці, виборі, описі, конструюванні, створенні й придбанні засобів системи з метою дотримання правил безпеки.

На СІБ зазвичай покладається виконання й інших обов'язків, які стосуються створення власне СЗІ, а саме:

- формування вимог до СЗІ в процесі створення СППР;
- участь у проектуванні СЗІ, її випробуваннях і прийманні в експлуатацію;
- планування, організація і забезпечення функціонування СЗІ в процесі функціонування СППР;
- розподіл між користувачами СППР необхідних реквізитів захисту;
- спостереження за функціонуванням СЗІ і її елементів;
- організація перевірок надійності функціонування СЗІ;
- вживання заходів при спробах НСД до інформації і при порушеннях правил функціонування СЗІ.

Для виконання покладених задач СБІ повинна мати відповідний організаційно-правовий статус, а саме:

- чисельність СІБ повинна бути достатньої для виконання всіх перерахованих функцій;
- СІБ повинна підпорядковуватись тієї особі, що несе на підприємстві персональну відповідальність за дотримання правил поводження з інформацією, що захищається;
- штатний склад СІБ не повинний мати інших обов'язків, не пов'язаних з функціонуванням СППР;
- співробітники СІБ повинні мати право доступу в усі приміщення, де встановлена апаратура СППР і право припиняти автоматизовану обробку інформації при наявності безпосередньої загрози для інформації, що захищається;
- керівнику СІБ має бути надано право забороняти включення в число діючих нові елементи СППР, якщо вони не відповідають вимогам захисту інформації;
- для СІБ повинні бути створені всі умови, необхідні для виконання її функцій.

У структуру СІБ можуть входити такі підрозділи (всі або окремі з них):

- група режиму;
- служба охорони;
- пожежна охорона;

- аналітична група;
- детективна група (спостереження за співробітниками);
- група протидії технічній розвідки;
- група протидії НСД;
- криптографічна група.

Очолювати СІБ має особа, безпосередньо підлегла керівнику підприємства (або він самий повинен бути директором чи заступником директора). У нього повинен бути заступник начальника служби безпеки. До складу підрозділів СІБ можуть входити аналітики, юристи, фахівці в сфері забезпечення безпеки, економічної розвідки, промислової контррозвідки, технічні фахівці, що вміють застосовувати спеціальну техніку для захисту приміщень, а також співробітники фізичної охорони і пропускного режиму.

Зрозуміло, що не кожному підприємству під силу нести витрати із забезпечення ефективної служби безпеки (адже на утримання служб безпеки може виділятися до 20% чистого прибутку підприємства за рік), та й не для будь-якої СППР потрібні вищеперераховані заходи. Тому, насамперед, необхідно провести економічне обґрунтування створення СІБ, виходячи з функціоналу і масштабу СППР. Іноді економічно виправданим для невеликих систем з метою забезпечення безпеки залучати спеціалізовані організації, за допомогою яких професійно визначається обсяг послуг щодо захисту інформації і приймаються необхідні міри.

	Замислитись про створення служби безпеки необхідно відразу, як тільки виявляється реальна небезпека системі (можливий витік «закритої» інформації, нанесення матеріального чи фінансового збитку, інші загрози), та якщо обсяг зведень, що складають комерційну таємницю, є значним.

Контрольні запитання та завдання

1. Сформулюйте основні архітектурні принципи кібербезпеки СППР.
2. Поясніть основні компоненти загальної структури захищеної СППР.
3. Дайте визначення основних рівнів забезпечення кібербезпеки СППР.
4. Назвіть головні принципи формування системи захисту інформації (СЗІ).
5. Поясніть призначення служби інформаційної безпеки (СІБ) на підприємстві.

2.2. ІНЖЕНЕРНО-ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ В СППР

Основні поняття Інженерно-технічного рівня інформаційної безпеки.
Технічні канали витоку.
Охоронні системи.

2.2.1. Основні поняття інженерно-технічного захисту СППР

Безпека СППР залежить від оточення, у якому вона функціонує. Тому необхідним є вжиття заходів для захисту будинків і прилеглої території, підтримуючої інфраструктури, обчислювальної техніки, носіїв даних. Такі заходи відносяться до *інженерно-технічних* (іноді їх ще називають фі*зичними*).

Основний принцип фізичного захисту, дотримання якого варто постійно контролювати, формулюється як «безперервність захисту в просторі й часі». Іншими словами, для фізичного захисту вікон небезпеки не повинно бути.

До напрямків інженерно-технічного захисту відносяться наступні:

- керування доступом у приміщення;
- протипожежні заходи;
- захист підтримуючої інфраструктури;
- захист від електромагнітного перехоплення даних;
- захист мобільних (пересувних) елементів системи.

До основних організаційних заходів інженерно-технічного захисту відносяться:

- розробка і затвердження функціональних обов'язків посадових осіб служб інженерно-технічного захисту;
- внесення необхідних змін і доповнень в усі організаційно-розпорядницькі документи (положення про підрозділи, обов'язки посадових осіб і т.ін.) з урахуванням питань забезпечення інженерно-технічного захисту і дій у випадку виникнення кризових ситуацій;
- оформлення юридичних документів (договорів, наказів і розпоряджень керівництва організації) з питань регламентації відносин з працівниками, що працюють в сфері інженерно-технічного захисту системи;
- розробка науково-технічних і методологічних основ інженерно-технічного захисту СППР;
- забезпечення виключення можливості таємного проникнення в приміщення, установки апаратури, що прослуховує, і т.ін.);

- перевірка і сертифікація використовуваних в СППР технічних і програмних засобів на предмет визначення заходів для їхнього захисту від витоку по каналах побічних електромагнітних випромінювань і наведень (ПЕВМН);
- визначення порядку призначення, зміни, затвердження і надання конкретним посадовим особам необхідних повноважень з доступу до приміщень СППР;
- виявлення найбільш ймовірних загроз для даної СППР, виявлення уразливих місць інженерно-технічного захисту, каналів доступу;
- оцінка можливого збитку, викликаного порушенням безпеки інформації, розробка адекватних вимог по основних напрямках інженерно-технічного захисту;
- організація надійного перепускного режиму;
- визначення порядку обліку, видачі, використання і збереження знімних магнітних носіїв інформації, що містять еталонні і резервні копії програм і масивів інформації, архівні дані і т.ін.
- явний і схований контроль за роботою персоналу системи;
- організація обліку, збереження, використання і знищення документів і носіїв із закритою інформацією;
- визначення переліку необхідних заходів для забезпечення безупинної роботи СППР і діях персоналу під час стихійних явищ і т.ін.;
- контроль функціонування і керування використовуваними засобами захисту;
- періодичний аналіз стану й оцінка ефективності заходів інженерно-технічного захисту.

Важливою складовою інженерно-технічного захисту є роботи з *технічного захисту інформації* (ТЗІ). Вони передбачають:

- категорування об'єктів захисту;
- включення до технічних завдань на монтаж в СППР електронно-обчислювальної техніки (ЕОТ) розділу з ТЗІ;
- монтаж ЕОТ відповідно до рекомендацій цього документа;
- обстеження (в тому числі технічний контроль) об'єктів СППР;
- установлення (при необхідності) атестованих технічних засобів захисту;
- технічний контроль за ефективністю вжитих заходів.

Для ЕОТ, що обробляє інформацію з обмеженим доступом (ІзОД), проводиться обов'язкове категорування згідно з чинним Положенням про категорування. Обсяг і зміст робіт із захисту цієї інформації визначаються присвоєною категорією.

Обстеження СППР відповідно до рекомендацій цього документа проводиться структурними підрозділами СБІ, у віданні яких знаходиться система, або підприємствами, установами, організаціями і громадянами, що одержали в установленому порядку відповідні ліцензії державного органу з питань технічного захисту інформації. Рекомендований алгоритм обстеження містить такі процедури:

- аналіз у технічних засобах ЕОТ потоків інформації з обмеженим доступом;
- визначення складу кабельних ліній, що виходять за межі території, що контролюється і мають паралельний пробіг з кабелями СППР;
- виявлення комунікацій, що проходять через територію СППР і мають вихід за її межі;
- інструментальне вимірювання інформативних побічних електромагнітних випромінювань та наводок;
- оцінку відповідності рівнів сигналів і параметрів полів, які є носіями ІзОД, нормам ефективності захисту.

За результатами обстеження складається акт, в якому відбиваються категорія об'єктів, їх перелік (найменування, тип, заводський номер), перелік комунікацій, оцінка відповідності монтажу цим рекомендаціям, пропозиції щодо застосування додаткових заходів захисту (при необхідності). До акта додаються схема розміщення технічних засобів і проходження комунікацій на ньому та протоколи вимірювань.

2.2.2. Технічні канали витоку інформації в СППР

Носіями інформації в СППР є електричні й електромагнітні поля й сигнали, що утворюються в результаті роботи технічних засобів обробки інформації. У процесі функціонування засобів ЕОТ в конструктивних елементах і кабельних з'єднаннях циркулюють електричні струми інформативних сигналів, у результаті чого формуються електромагнітні поля, рівні яких можуть бути достатніми для прийому сигналів і добування інформації за допомогою спеціальної апаратури. При цьому інформативні сигнали можуть поширюватися на великі відстані й реєструватися засобами технічних розвідок і за межами контрольованої території.

Крім електромагнітних коливань джерелами утворення каналів витоку можуть бути різні акустичні перетворювачі. Але найбільшу небезпеку з погляду витоку інформації представляють побічні (паразитні, ненавмисні) випромінювання технічних засобів, що беруть участь у процесі передачі, обробки й зберігання таємної інформації. Небезпечним є й вплив небажа-

ного сигналу на засоби обробки відкритої інформації й на системи життєзабезпечення.

Перехоплення даних з використанням технічних каналів витоку може здійснюватися різними способами. Зловмисник може підглядати за екраном монітора, читати пакети, передані по мережі, робити аналіз випромінювань і т.д. Залишається уповати на повсюдне використання криптографії, намагатися максимально розширити контрольовану територію, використовувати приміщення для системи на відстані від інших будинків, створювати спеціальні захищені приміщення, намагатися тримати під контролем лінії зв'язку (наприклад, укладати їх у надувну оболонку з виявленням проколювання). Але ці заходи мають, звичайно, погоджуватись з вимогами рівня конфіденційності у порівнянні з іншими завданнями СППР.

Витік по каналах побічних електромагнітних випромінювань і наведень (ПЕМВН) – можливість доступу до інформації в СППР, що здійснюється шляхом перехоплення й відповідної обробки побічних (паразитних, ненавмисних) випромінювань технічних засобів передачі інформації, використовуваних у зазначеній системі для збору, обробки, зберігання й обміну інформацією.

Засоби перехоплення можуть бути представлені у вигляді комплексу, що містить приймальний пристрій, погоджувальний фільтр і аналізатор, що забезпечують відповідно виявлення й найкращі умови для виділення випромінювання, яке цікавить порушника, оптимальну обробку даного виду сигналу з перешкодою з метою поліпшення «зрозумілості» сигналу й прийняття рішення, що забезпечує граничну «розбірливість» сигналу. При цьому аналіз зареєстрованого сигналу може проводитися багаторазово з використанням методів обробки сигналів на ПК.

На цей час склалася система захисту об'єктів від витоку інформації, що включає проведення організаційних, організаційно-технічних, технічних заходів і заходів щодо контролю за виконанням захисту. Остаточний висновок про ефективність заходів щодо технічного захисту інформації дається за результатами інструментального контролю.

Які ж існують рекомендації із захисту інформації від ПЕМВН?

За загальними рекомендаціями навколо СППР має забезпечуватися контрольована територія (КТ), за межами якої відношення «інформативний сигнал/шум» не повинне перевищувати норми. З цією метою об'єкти захисту СППР рекомендується розташовувати у внутрішніх приміщеннях, бажано, на нижніх поверхах. При наявності таємної інформації високоча-

стотні (ВЧ) технічні засоби – до яких, як правило, відносяться комп'ютери та інші пристрої – рекомендується розміщувати в екранованих приміщеннях (капсулах).

У відповідності до рекомендацій із захисту інформації від перехоплення наводок на незахищені технічні засоби, що мають вихід за межі КТ, у незахищених каналах зв'язку, лініях, проводах та кабелях встановлюються завадозаглушувальні фільтри. Проводи і кабелі прокладаються в екранованих конструкціях. Монтаж кіл технічних засобів, що мають вихід за межі КТ, рекомендується проводити екранованим кабелем або прокладеним в екранувальних конструкціях.

Рекомендації із захисту інформації від витоку колами заземлення пропонують, щоб система заземлення технічних засобів не мала виходу за межі КТ і повинна розміщуватися на відстані не менше 10-15 м від них. Заземлювальні проводи повинні бути виконані з мідного дроту (кабелю) з перехідним опором з'єднань не більше 600 мкОм. Опір заземлення не повинен перевищувати 4 Ом.

Існують витоки інформації колами електроживлення. Відповідними рекомендаціями із захисту найбільш ефективно гальванічну та електромагнітну розв'язку кабелів електроживлення від промислової мережі забезпечує їх розділова система типу «електродвигун-генератор». Електроживлення допускається також здійснювати через завадозаглушувальні фільтри. Електроживлення повинно здійснюватись екранованим (броньованим) кабелем.

У випадках, коли пасивні заходи не забезпечують необхідної ефективності захисту об'єктів, рекомендується застосовувати системи просторового зашумлення об'єктів. Встановленню підлягають тільки засоби, сертифіковані відповідною державною службою з питань технічного захисту інформації.

До ефективних засобів захисту відносяться обладнання та застосування екранувальних конструкцій. Основні рекомендації пропонують, щоб екранувальні кабельні конструкції разом з екранувальними конструкціями технічних засобів створювали екранувальний замкнений об'єм.

2.2.3. Охоронні системи

Засоби фізичного керування доступом на територію і в приміщення відомі давно. Це охорона, двері із замками, перегородки, телекамери, датчики руху й багато чого іншого. Для вибору оптимального (за критерієм вартість/ефективність) засобу доцільно провести аналіз існуючих ризиків. Крім того, є сенс періодично відслідковувати появу технічних новинок у даній галузі, намагаючись максимально автоматизувати фізичний захист.

При проектуванні й реалізації заходів фізичного керування доступом доцільно застосовувати об'єктний підхід. По-перше, визначається *периметр безпеки*, що обмежує контрольовану територію (рис. 2.5). На цьому рівні деталізації важливо продумати зовнішній інтерфейс організації – порядок входу/виходу штатних співробітників і відвідувачів, внесення/виносу техніки. Усе, що не входить у зовнішній інтерфейс, повинне бути інкапсульоване, тобто захищене від нелегальних проникнень.

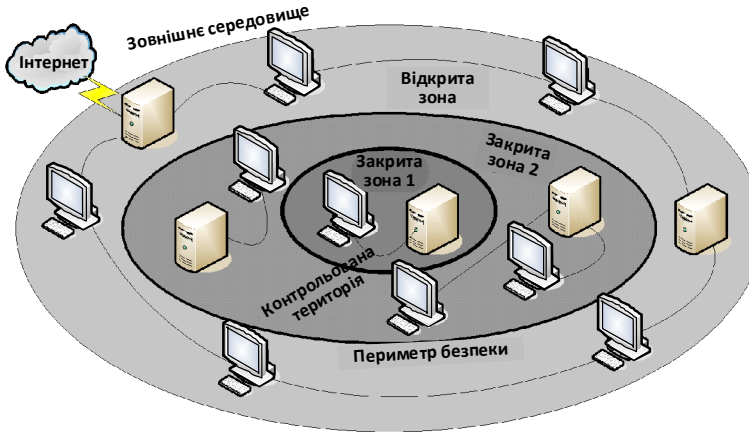


Рис. 2.5. Периметр безпеки і декомпозиція контрольованої території

По-друге, здійснюється *декомпозиція контрольованої території,* виділяються об'єкти й зв'язки (проходи) між ними. При такій, більш глибокій деталізації, варто виділити серед об'єктів найбільш критичні з погляду безпеки й забезпечити їм підвищену увагу. Декомпозиція повинна бути змістовно виправданою, що забезпечує розмежування різнорідних сутностей, таких як обладнання різних власників або персонал, що працює з даними різного ступеня критичності.

Важливо зробити так, щоб відвідувачі, по можливості, не мали безпосереднього доступу до комп'ютерів або, у крайньому випадку, подбати про те, щоб від вікон і дверей не проглядалися екрани моніторів і принтери. Необхідно, щоб відвідувачів за зовнішнім виглядом можна було відрізнити від співробітників. Для цього відвідувачам видаються ідентифікаційні картки.

Крім візуального спостереження, доцільно, щоб ці картки використовувались й для керування доступом в приміщення з використанням відповідних технічних засобів – рідерів. Основні вимоги до такої системи ідентифікації полягають в однозначності розпізнавання користувача по унікаль-

ним, властивим йому одному ознакам. Однією з найперспективніших і таких, що активно розвивається є ідентифікація з використанням біометрії, наприклад ідентифікації по відбитках пальців і зображенню обличчя. Про ці та інші технології ідентифікації будемо говорити у наступному розділі.

Важливим засобом інформування про порушення контрольованої території є системи *охоронної сигналізації*. Вони класифікуються як автономні та централізовані. Перші подають сигнал тривоги на місці встановлення. Другі передбачають наявність центрального пульту, на якому відображується стан об'єкту, що отримується від датчиків, встановлених на об'єктах, що охороняються. У системах захисту територій використовуються мікрохвильові, інфрачервоні, ємнісні, електричні та інші датчики. Незважаючи на притаманні таким системам недоліки і відносно значні витрати на утримання та розвиток, вони знайшли дуже широке поширення.

Без перебільшення можна сказати, що історія людства тісно пов'язана з *пожежами*. На жаль, пожежі, як і раніше, трапляються часто й завдають великої шкоди і в наші часи. Методи запобігання й боротьби з вогнем добре розроблені, написані томи протипожежних інструкцій. Для нас важливо відзначити необхідність установки протипожежної сигналізації й автоматичних засобів пожежогасіння в приміщеннях розташування засобів СППР.

Системи електро-, водо- і теплопостачання, кондиціонери й засоби комунікацій відносяться до *підтримуючої інфраструктури*. До них застосовні ті ж вимоги цілісності й доступності, що й до інформаційних систем. Для забезпечення цілісності потрібно захищати обладнання від крадіжок і ушкоджень. Для підтримки доступності варто вибирати надійне обладнання (з максимальним часом наробітку на відмову), дублювати відповідальні вузли й завжди мати під рукою запчастини. А співробітники повинні знати, куди варто звертатися при виявленні аварій.

Контрольні запитання та завдання

1. Сформулюйте основні принципи фізичного (інженерно-технічного) захисту СППР.
2. Поясніть основні компоненти загальної структури контрольованої території СППР.
3. У чому полягають роботи з технічного захисту інформації (ТЗІ)?
4. Назвіть основні види технічних каналів витоку інформації в СППР.
5. Роз'ясніть сутність рекомендацій із захисту інформації від ПЕМВН.
6. Поясніть призначення та види засобів охорони на підприємстві, де експлуатується СППР.

7. У чому полягають особливості підтримуючої інфраструктури с точки зору безпеки СППР?

2.3. ЗАКОНОДАВЧИЙ РІВЕНЬ, СТАНДАРТИ І СПЕЦИФІКАЦІЇ КІБЕРБЕЗПЕКИ

Огляд українського та закордонного законодавства в сфері інформаційної безпеки. Оцінні стандарти й технічні специфікації. «Оранжева книга» як оцінний стандарт.
Інформаційна безпека розподілених систем. Гармонізовані критерії Європейських країн.

2.3.1. Огляд українського та закордонного законодавства в сфері інформаційної та кібербезпеки

Як вже вказувалось, у сфері забезпечення інформаційної безпеки успіх може принести тільки комплексний підхід, для чого необхідно поєднувати заходи різних рівнів – адміністративного, процедурного, організаційно-технічного. Серед них найважливішим для забезпечення безпеки вважається законодавчий рівень. Адже, як відомо, значну кількість людей втримує від протиправних дій усвідомлення того, що це засуджується й/або карається суспільством, або тому, що так робити не прийнято. З іншого боку, державний контроль створює умови для скоординованого розвитку засобів захисту та сприяє запобіганню «самодіяльності» у цій сфері. Тому на законодавчому рівні розрізняють дві групи заходів, які важливі рівною мірою:

- заходи, спрямовані на створення й підтримку в суспільстві негативного відношення до порушень і порушників інформаційної та кібербезпеки (заходи обмежувальної спрямованості);
- напрямні й координуючі заходи, що сприяють підвищенню освіченості фахівців в галузі безпеки, які допомагають у розробці й поширенні засобів забезпечення безпеки (заходи будівничої спрямованості).

Найважливіше на законодавчому рівні – це узгодити процес розробки нормативних актів з розвитком інформаційних технологій, щоб відставання не було занадто великим.

З початку «комп'ютерної ери» у світі було напрацьовано чимало нормативних документів. Й в Україні за часи незалежності прийнято низку законів, що торкаються питань інформаційної та кібербезпеки, а саме:

«Про інформацію»;

«Про основи національної безпеки України»;

«Про захист інформації в інформаційно-телекомунікаційних системах»;

«Про державну таємницю»;

«Про наукову і науково-технічну експертизу»;

«Про ліцензування певних видів господарської діяльності»;

«Про електронний цифровий підпис»;

«Про електронний документ та електронний документообіг»;

«Про захист персональних даних»;

«Про доступ до публічної інформації»;

«Про Національну систему конфіденційного зв'язку»;

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

Основним законом України є Конституція, стаття 23 якої гарантує право на таємницю листування, телефонних переговорів, поштових, телеграфних і інших повідомлень, а стаття 29 – право вільно шукати, одержувати, передавати, виробляти й поширювати інформацію будь-яким законним способом.

Сучасна інтерпретація цих положень включає забезпечення конфіденційності даних, у тому числі в процесі їхньої передачі по комп'ютерних мережах, а також доступ до засобів захисту інформації.

Названі закони виділяють такі цілі захисту інформації, як запобігання витоку, розкрадання, втрати, перекручування, підробки інформації; запобігання інших форм незаконного втручання в інформаційні ресурси й інформаційні системи, забезпечення правового режиму документованої інформації як об'єкта власності; забезпечення прав суб'єктів в інформаційних процесах і при розробці, виробництві й застосуванні інформаційних систем, технологій і засобів їхнього забезпечення.

Досить просунутим у плані інформаційної та кібербезпеки є Кримінальний кодекс України (ККУ), який у главі 28 – «Злочини в сфері комп'ютерної інформації» – містить три статті – стаття 272. Неправомірний доступ до комп'ютерної інформації; стаття 273. Створення, використання й поширення шкідливих програм для ЕОМ; стаття 274. Порушення правил експлуатації ЕОМ, системи ЕОМ або їхньої мережі.

Крім Законів, в сфері кібербезпеки діє низка указів та розпоряджень, виданих Президентом України. Серед них слід відмітити такі:

«Про Положення про порядок здійснення криптографічного захисту інформації в Україні» від 22.05.98 № 505;

«Про Положення про технічний захист інформації в Україні» від 27.09. 99 № 1229;

«Про заходи щодо забезпечення розвитку і функціонування Національної системи конфіденційного зв'язку» від 15.01.2003 №7;

«Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України» від 26.05.2015 № 287;

«Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» від 15.03.2016 № 96.

На виконання зазначених законів та указів Кабінет Міністрів України видав низку постанов, серед яких слід назвати такі:

«Про затвердження Концепції технічного захисту інформації в Україні» від 08.10.97 №1126;

«Про затвердження переліку обов'язкових етапів робіт під час проектування, впровадження та експлуатації систем та засобів автоматизованої обробки та передачі даних» від 04.02.1998 №121;

«Про затвердження Порядок акредитації центру сертифікації ключів» від 13.07.2004 №903;

«Про затвердження Порядок застосування електронного цифрового підпису органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності» від 28.10.2004 №1452;

«Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» від 29.03.2006 №373.

Державною службою спеціального зв'язку та захисту інформації України у різні роки розроблено низку нормативних документів (НД) у сфері технічного та криптографічного захисту інформації: з технічного захисту інформації в комп'ютерних (автоматизованих) системах від несанкціонованого доступу (НД ТЗІ), щодо захисту інформації від витоку каналами ПЕМВН та ін.

Що стосується закордонного законодавства в галузі інформаційної та кібербезпеки ми лише поверхово окреслимо деякі закони кількох країн, оскільки, наприклад, тільки в США таких законодавчих актів діє близько 500.

Серед них ключову роль відіграє американський «Закон про комп'ютерну безпеку» (Computer Security Act), прийнятий ще 1987 року. Його метою була реалізація мінімально достатніх дій із забезпечення безпеки

інформації у федеральних комп'ютерних системах. Важливим положення цього акту стало те, що у ньому вказується конкретний виконавець – Національний інститут стандартів і технологій (НІСТ), відповідальний за випуск стандартів і посібників, спрямованих на захист від знищення й несанкціонованого доступу до інформації, а також від крадіжок і підробок, що здійснюються за допомогою комп'ютерів.

У 1997 році з'явилося продовження цього закону – «Про вдосконалювання інформаційної безпеки» (Computer Security Enhancement Act), спрямований на посилення ролі НІСТ і спрощення операцій із криптозасобами. Важливо, що було введене поняття програми безпеки, що передбачає економічно виправдані захисні міри й синхронізацію з життєвим циклом АС, що потім згадується в законодавстві США неодноразово.

У законодавстві Німеччини слід виділити досить розгорнутий Закон про захист даних (Federal Data Protection Act), цілком присвячений захисту персональних даних.

2.3.2. Оцінні стандарти і технічні специфікації

Фахівцям в галузі кібербезпеки сьогодні практично неможливо обійтися без знань відповідних стандартів і специфікацій. На це є декілька причин. Одна з них – формальна – полягає у тому, що необхідність слідуванню деяким стандартам (наприклад, криптографічним) закріплена законодавчо. Однак найбільш переконливі змістовні причини. По-перше, стандарти і специфікації – це одна з форм нагромадження знань, насамперед про програмно-технічний рівні кібербезпеки. У них зафіксовані апробовані, високоякісні рішення і методології, розроблені найбільш кваліфікованими фахівцями. По-друге, й ті, й інші є основним засобом забезпечення взаємної сумісності апаратно-програмних систем та їхніх компонентів.

Оцінні стандарти спрямовані на класифікацію АС і засобів захисту у відповідності до вимог безпеки. У свою чергу технічні специфікації регламентують різні аспекти реалізації засобів захисту. Важливо відзначити, що між цими видами нормативних документів немає глухої стіни. Оцінні стандарти виділяють найважливіші, з погляду безпеки, архітектурні аспекти АС, а інші технічні специфікації визначають, як будувати АС запропонованої архітектури.

Роботи зі стандартизації були розпочаті Міжнародною організацією стандартизації (ISO) ще з 1980 року. Зараз в неї працює спеціальний підкомітет TC97/SC20. У Європейському інституті стандартів з телекомунікацій (ETSI) ведеться велика робота зі стандартизації засобів безпеки при пере-

дачі інформації різними каналами. Працює консультативна група з методів забезпечення безпеки STAG, що готує технічні звіти та проекти стандартів.

З оцінних перш за все необхідно виділити стандарт Міністерства оборони США «Критерії оцінки довірених комп'ютерних систем» і його інтерпретацію для мережних конфігурацій, «Гармонізовані критерії Європейських країн», міжнародний стандарт «Критерії оцінки безпеки інформаційних технологій» і Федеральний стандарт США «Вимоги безпеки для криптографічних модулів".

Технічні специфікації, застосовні до сучасних розподілених АС, створюються, головним чином, «Тематичною групою по технології Інтернет» (*Internet Engineering Task Force, IETF*) і її підрозділом – робочою групою з безпеки. Ядром розглянутих технічних специфікацій служать документи по безпеці на IP-рівні (*IPsec*). Крім цього, аналізується захист на транспортному рівні (*Transport Layer Security, TLS*), а також на рівні додатків (*специфікації GSS-API, Kerberos*).

У питаннях мережної безпеки неможливо розібратися без освоєння специфікацій X.800 «Архітектура безпеки для взаємодії відкритих систем», X.500 «Служба директорій: огляд концепцій, моделей і сервісів» і X.509 «Служба директорій: каркаси сертифікатів відкритих ключів і атрибутів».

Британський стандарт BS 7799 «Управління інформаційною безпекою. Практичні правила» є корисним для керівників організацій і осіб, відповідальних за інформаційну безпеку. Його положення без скількинебудь істотних змін відтворені у міжнародному стандарті ISO/IEC 17799.

Історично першим оцінним стандартом, що отримав широке поширення й зробив величезний вплив на базу стандартизації кібербезпеки у багатьох країнах, став стандарт Міністерства оборони США «Критерії оцінки довірених комп'ютерних систем» (*Department of Defense Trusted Computer System Evaliation Criteria, TCSEC*). Цей документ, що найчастіше з-за кольору обкладинки називається «Оранжевою книгою», був уперше опублікований у серпні 1983 року. Вже одна назва стандарту вимагає коментаря. Мова йде не про *безпечн*і, а про *довірені системи*, тобто системи, яким можна надати певного ступеня довіри. Очевидно, що абсолютно безпечних систем не існує, це абстракція. Є смисл оцінювати лише ступінь довіри, якої можна надати тій або іншій системі.

«Оранжева книга» пояснює поняття безпечної системи, що «управляє, за допомогою відповідних засобів, доступом до інформації, так, що тільки належним чином авторизовані особи або процеси, що діють від їхнього імені, отримують право читати, записувати, створювати й вилучати інформацію».

У цьому документі довірена система визначається як «система, що використовує достатні апаратні й програмні засоби, щоб забезпечити одночасну обробку інформації різного ступеня таємності групою користувачів без порушення прав доступу».

Треба звернути увагу, що в розглянутих Критеріях і безпека, і довіра оцінюються винятково з погляду керування доступом до даних, що є одним із засобів забезпечення конфіденційності й цілісності.

Але найголовніше, що в документі уведені два основних критерії, за якими оцінюється ступінь довіри. По-перше, це *політика безпеки* – набір законів, правил і норм поведінки, що визначають, як організація обробляє, захищає й поширює інформацію. По-друге, це *рівень гарантованості* як міра довіри, що може бути надана архітектурі й реалізації АІС. Залежно від сформульованої політики вибираються конкретні *механізми забезпечення безпеки*.

Важливим засобом забезпечення безпеки є *механізм підзвітності* (протоколювання). Довірена система повинна фіксувати всі події, що стосуються безпеки. Ведення протоколів повинне доповнюватися *аудитом*, тобто аналізом реєстраційної інформації.

Узагальненням світового досвіду в організації керування інформаційною безпекою є стандарт ISO/IEC 27001:2005 *Information security management systems*. Він, як і ряд інших «безпечних» стандартів – це набір кращих практик, тобто в їхній основі лежить отримана в реальному житті віддача від впровадження тих або інших захисних технологій або заходів.

ISO 27001 визначає загальну організацію, напрямки планування, використання оцінки ризику, оцінки ефективності, контролю поліпшень і т.ін. у контексті інформаційної безпеки. Ключовою відмінністю цього стандарту є процесний підхід, тобто положення про те, що сертифікується *процес*, а не система захисту. І якщо за цим стандартом на підприємстві сертифікований один або декілька процесів, але існує ще множина інших процесів, то вони можуть стати тими самими слабкими ланками у захисті. Однак ця гнучкість і універсальність стандарту робить його одночасно й складним у впровадженні для більшості підприємств.

Серед оцінних стандартів найповнішим є міжнародний стандарт «Критерії оцінки безпеки інформаційних технологій», виданий 1999 року. Він став підсумком майже десятилітньої роботи фахівців декількох країн, він увібрав у себе досвід існуючих на той час документів національного й міжнаціонального масштабу. З історичних причин даний стандарт часто називають «Загальними критеріями» (або навіть ЗК).

«Загальні критерії» насправді є метастандартом, що визначає інструменти оцінки безпеки АІС і порядок їхнього використання, виходячи *з вимог безпеки*, що існують для конкретної організації й/або конкретної АІС.

Типовий набір вимог, яким повинні задовольняти продукти й/або системи певного класу (наприклад, операційні системи на комп'ютерах в урядових організаціях) являє *профіль захищеності*. Сукупність вимог до конкретної розробки, виконання яких забезпечує досягнення поставлених цілей безпеки, містить *завдання по безпеці*. У ЗК об'єкт оцінки розглядається в контексті *середовища безпеки*, що характеризується певними умовами й загрозами.

Дуже важливо, що безпека в ЗК розглядається не статично, а в прив'язці до життєвого циклу об'єкта оцінки. Виділяються такі етапи, як визначення призначення, умов застосування, цілей і вимог безпеки, проектування та розробка, випробування, оцінка і сертифікація, впровадження й експлуатація.

Досить передовим стандартом, який створив передумови для появи «Загальних критеріїв», є Гармонізовані критерії Європейських країн, що були опубліковані 1991 року від імені відповідних органів чотирьох країн – Франції, Німеччини, Нідерландів і Великобританії.

Принципово важливою рисою Європейських Критеріїв є відсутність вимог до умов, у яких повинна працювати АС. Так званий *спонсор*, тобто організація, що запитує сертифікаційні послуги, формулює мету оцінки, тобто описує умови, у яких повинна працювати система, можливі загрози її безпеки й надавані нею захисні функції. Завдання органа сертифікації – оцінити, наскільки повно досягаються поставлені цілі, тобто наскільки коректні й ефективні архітектура й реалізація механізмів безпеки в описаних спонсором умовах.

Згідно з термінологією «Оранжевої книги», Європейські Критерії відносяться до гарантованості безпечної роботи системи. Вимоги до політики безпеки і наявності захисних механізмів не є складовою частиною Критеріїв. Втім, щоб полегшити формулювання мети оцінки, Критерії містять як додаток опис десяти класів функціональності, типових для урядових і комерційних систем.

2.3.3. Кібербезпека розподілених систем

На перше місце серед технічних специфікацій кібербезпеки розподілених систем варто поставити документ X.800 «Архітектура безпеки для взаємодії відкритих систем», який з'явився трохи пізніше «Оранжевої кни-

ги». В ньому виділені найважливіші мережні сервіси безпеки: автентифікація, керування доступом, забезпечення конфіденційності й/або цілісності даних, а також неможливість відмовитися від зроблених дій. Для реалізації сервісів передбачені наступні мережні механізми захисту і їхні комбінації: шифрування, електронний цифровий підпис, керування доступом, контроль цілісності даних, керування маршрутизацією та ін. Обрано рівні еталонної семирівневої моделі (модель побудови мережного відкритого середовища), на яких можуть бути реалізовані сервіси і механізми захисту. Нарешті, детально розглянуті питання адміністрування засобів безпеки для розподілених конфігурацій.

Сервіси мережевої безпеки і ролі, що ними виконуються, виділяють наступним чином.

Автентифікація. Даний сервіс забезпечує перевірку дійсності партнерів по спілкуванню й перевірку дійсності джерела даних. Автентифікація використовується при встановленні з'єднання й, можливо, періодично під час сеансу.

Керування доступом. Забезпечує захист від несанкціонованого використання ресурсів, доступних по мережі.

Конфіденційність даних. Забезпечує захист від несанкціонованого одержання інформації. Окремо згадується ***конфіденційність трафіку*** (захист інформації, яку можна одержати, аналізуючи мережні потоки даних).

Цілісність даних підрозділяється на підвиди залежно від того, який тип спілкування використовують партнери – із установленням з'єднання або без нього, чи захищаються всі дані або тільки окремі поля, чи забезпечується відновлення у випадку порушення цілісності.

Неспростовність (неможливість відмовитися від зроблених дій) забезпечує два види послуг: неспростовність із підтвердженням дійсності джерела даних і неспростовність із підтвердженням доставки. Побічним продуктом неспростовності є *автентифікація джерела даних*.

Відповідно до рекомендацій X.800, *адміністрування* засобів мережевої безпеки містить у собі поширення інформації, необхідної для роботи сервісів і механізмів безпеки, а також збір і аналіз інформації про їхнє функціонування. Прикладами можуть служити поширення криптографічних ключів, установка значень параметрів захисту, ведення реєстраційного журналу й т.п.

Концептуальною основою адміністрування є інформаційна база керування безпекою. Ця база може не існувати як єдине (розподілене) сховище, але кожна з кінцевих систем повинна мати інформацію, необхідну для реалізації вибраної політики безпеки.

У 1987 році у США була опублікована інтерпретація «Оранжевої книги» для мережних конфігурацій. Даний документ складається із двох частин. Перша містить власне інтерпретацію, у другий розглядаються сервіси безпеки, специфічні або особливо важливі для мережних конфігурацій. Найважливіше з введених нових понять – *мережна довірена обчислювальна база* як розподілений аналог довіреної обчислювальної бази ізольованих систем. Інший принциповий аспект – *облік динамічності мережних конфігурацій*.

Мережна довірена обчислювальна база формується із всіх частин всіх компонентів мережі, що забезпечують інформаційну безпеку. Довірена мережна система повинна забезпечувати такий розподіл захисних механізмів, щоб загальна політика безпеки реалізовувалася, незважаючи на уразливість комунікаційних шляхів і на паралельну, асинхронну роботу компонентів.

Інтерпретація відрізняється від самих «Критеріїв» обліком динамічності мережних конфігурацій. Передбачається наявність засобів перевірки дійсності й коректності функціонування компонентів перед їхнім включенням у мережу, наявність протоколу взаємної перевірки компонентами коректності функціонування один одного, а також присутність засобів оповіщення адміністратора про неполадки в мережі.

Серед захисних механізмів у мережних конфігураціях на першому місці стоїть криптографія, що допомагає підтримувати як конфіденційність, так і цілісність. Наслідком використання криптографічних методів є необхідність реалізації механізмів керування ключами.

Контрольні запитання та завдання

1. Назвіть основні українські законодавчі акти, що стосуються питань кібербезпеки.

2. Поясніть поняття оцінних стандартів та технічних специфіка-цій кібербезпеки.

3. У чому полягають особливості стандарту Міністерства обо-рони США «Критерії оцінки довірених комп'ютерних систем»?

4. Назвіть основну мету стандарту ISO/IEC 27001:2005 та метод її реалізації.

5. Роз'ясніть сутність рекомендацій документу X.800 «Архітек-тура безпеки для взаємодії відкритих систем».

6. Поясніть сутність поняття «мережна довірена обчислювальна база».

2.4. АДМІНІСТРАТИВНИЙ РІВЕНЬ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ СППР

Політика безпеки. Поняття і види політик безпеки. Програма безпеки. Управління ризиками.

2.4.1. Заходи адміністративного рівня

Заходи адміністративного рівня відносяться до заходів безпеки, які орієнтовані не лише на застосування технічних засобів, а й на людей. Адже, як вказувалося, саме люди виявляються головною загрозою кібербезпеки, тому «людський чинник» заслуговує на особливу увагу.

Варто чітко уявляти той ступінь залежності від сучасного рівня комп'ютерної обробки інформації, у якому знаходиться підприємство. Без перебільшення можна сказати, що на підприємстві необхідно створювати «інформаційну цивільну оборону». Персонал має бути у зоні постійної уваги керівництва та відповідних служб з огляду на забезпечення кібербезпеки.

Співробітникам потрібно роз'ясняти не тільки переваги, але й небезпеки, пов'язані з використанням інформаційних технологій. При цьому акцент варто робити не на кримінальному боці справи, а на цивільних аспектах, пов'язаних з підтримкою нормального функціонування підприємства та його автоматизованих систем завдяки надійної роботі апаратного й програмного забезпечення, тобто концентруватися на питаннях доступності й цілісності інформації, а за необхідності й її конфіденційності. Тому дії загального характеру, що вживаються керівництвом підприємства, й відносяться до адміністративного рівня забезпечення безпеки.

Головна мета заходів адміністративного рівня (рис. 2.6) – сформувати ***програму робіт*** з кібербезпеки й забезпечити її виконання, виділяючи необхідні ресурси й контролюючи стан справ. Основою цієї програми є ***політика безпеки,*** що відображає підхід підприємства до захисту своїх інформаційних ресурсів. У свою чергу політика безпеки будується на основі ***аналізу ризиків***, які визнаються реальними для даної СППР. Нарешті, до адміністративного рівня можна віднести й групу заходів, що іноді називаються процедурними, які пов'язані перш за все з управлінням персоналом, а також з підтримкою працездатності системи, реагуванням на порушення режиму безпеки, а також плануванням відбудовних робіт у разі якщо порушення безпеки призвело до руйнування системи.

У цьому комплексі заходів політика безпеки (ПБ) відіграє найважливішої ролі. Адже дотримання політики безпеки повинне забезпечити виконання того компромісу між альтернативами, що вибрали власники системи для її захисту. Вибір ПБ – це остаточне вирішення проблеми що є добре й що – погане в поводженні з цінною інформацією, яка обробляється в СППР. Після прийняття такого рішення можна будувати захист, тобто систему підтримки виконання правил ПБ. Таким чином, побудована система захисту інформації є гарною, якщо вона надійно підтримує виконання правил ПБ. Навпаки, система захисту інформації – погана, якщо вона ненадійно (не гарантовано) підтримує політику безпеки.

Рис. 2.6. Заходи адміністративного рівня

Підтримка необхідного рівня безпеки при розробці і проведенні в життя політики безпеки має забезпечуватись:

- контролем подій, що відбуваються в АС;
- обслуговуванням засобів захисту;
- періодичним контролем захищеності АС;
- моніторингом подій, що відбуваються в сфері інформаційної та кібербезпеки в державі та в світі.

Створення ПБ зазвичай складається з таких кроків. На першому визначається цінність інформації, алгоритмів і моделей, які використовуються в системі, та проводиться аналіз ризиків. На наступному кроці виписуються правила для процесів користування даними видами доступу до вказаних елементів, що мають оцінку цінності. Однак реалізація цих кроків є

складним завданням. Результатом помилкового або некоректного визначення правил ПБ зазвичай може бути руйнування цінної інформації без порушення політики. Таким чином, навіть гарна система захисту може бути «прозорою» для зловмисника при поганій ПБ.

Вирішення проблеми захищеності системи і інформації шляхом складання ПБ дозволяє залучити в теорію захисту точні математичні методи, тобто доводити, що дана система в заданих умовах підтримує ПБ. У цьому суть доказового підходу до захисту інформації, що дозволяє казати про «гарантовано захищену систему». Як вказувалося, формальне визначення політики безпеки називають математичною моделлю безпеки (див. розділ 1). Використання таких моделей дає змогу теоретично обґрунтувати відповідність системи захисту інформації вимогам заданої політики безпеки.

2.4.2. Поняття і види політик безпеки

При визначенні підходів до забезпечення кібербезпеки СППР, визначенні, як будуть захищатися програмно-апаратні й інформаційні ресурси, а також як повинні поводитися користувачі в тих або інших ситуаціях, адміністратори зіштовхуються з проблемою вибору на основі урахування принципів діяльності підприємства, де має функціонувати СППР, особливостей процесу прийняття рішень особою, що буде використовувати СППР, а також співвідношення важливості цілей і наявності ресурсів. Для того, щоб політика була успішною, важливо, щоб був обґрунтовано вибраний один напрямок із декількох можливих. Однак, коли рішення багатоальтернативне, то загальноприйнятого розуміння оптимальності важко знайти. Подібна ситуація існує в задачах захисту інформації, оскільки рішення про те, що інформація є захищеною, є неоднозначним. Крім того, система захисту – не самоціль, і повинна виконувати підлеглу функцію в порівнянні з головною метою СППР.

Результатом розв'язків в наведених ситуаціях є вибір правил розподілу й зберігання інформації, а також поводження з інформацією, що й називається ***політикою безпеки***.

Політика безпеки *(security policy)* – набір законів, правил і практичного досвіду, на основі яких будується керування, захист і розподіл критичної інформації.

Політика інформаційної безпеки – сукупність документів, що визначають управлінські й проектні рішення в сфері захисту інформації.

Термін «політика безпеки» є не зовсім точним перекладом англійського словосполучення *«security policy»*, однак у цьому випадку калька краще відбиває зміст цього поняття, ніж лінгвістично більш вірні «правила безпеки». Тим більш що мається на увазі не окремі правила або їхні набори, а стратегія організації кібербезпеки.

Отже, під політикою безпеки будемо розуміти сукупність документованих рішень, прийнятих керівництвом організації й спрямованих на захист інформації й асоційованих з нею ресурсів. Таке трактування, звичайно, набагато ширше, ніж набір правил розмежування доступу (саме це означав термін «security policy» в «Оранжевій книзі» і в побудованих на її основі нормативних документах інших країн).

Якщо згадати моделі захисту, розглянуті у першому розділі, то зміст політики безпеки дуже простий – це набір правил керування доступом. Стосовно регулювання доступів, то, як зазначалося, на сьогодні найкраще вивчені та знайшли застосування два основні види політики безпеки – дискреційна та мандатна. Останнім часом широко поширюється й нова модель доступу – *ролева політика*.

Відповідно до свого визначення в дискреційній політиці кожний об'єкт оголошується власністю відповідного користувача. Користувач, що є власником об'єкта, має усі права доступу до нього, а іноді й право передавати частину або усі права іншим користувачам. Крім того, власник об'єкта визначає права доступу інших суб'єктів до цього об'єкта, тобто політику безпеки відносно цього об'єкта.

Основне призначення повноважної (мандатної) політики безпеки – регулювання доступу суб'єктів системи до об'єктів з різним рівнем критичності і запобігання витоку інформації з верхніх рівнів посадової ієрархії на нижні, а також блокування можливого проникнення з нижніх рівнів на верхні. Для цього кожному об'єкту системи присвоюється рівень критичності, що визначає цінність інформації, яка міститься в ньому, а кожному суб'єкту системи присвоюється рівень прозорості, що визначає максимальне значення мітки критичності об'єктів, до яких суб'єкт має доступ. У тому випадку, коли сукупність міток має однакові значення, говорять, що вони належать до одного рівня безпеки. Організація міток має ієрархічну структуру і, таким чином, у системі можна реалізувати ієрархічно спадний потік інформації (наприклад, від рядових користувачів до керівництва). Чим важливіше об'єкт чи суб'єкт, тим вище його мітка критичності. Тому найбільш захищеними виявляються об'єкти з найбільш високими значеннями мітки критичності.

Повноважна політика безпеки була розроблена в інтересах Міноборони США для обробки інформації з різними грифами таємності. Її засто-

сування в комерційному секторі стримується такими основними причинами, як відсутність чіткої класифікації збереженої й оброблюваної інформації, аналогічної державної класифікації (грифи таємності), а також значна вартість реалізації і накладних витрат.

Щоб правильно розмежувати доступ, треба розуміти, хто із користувачів хоче виконати дію і чи може він це зробити. Серед підходів до вирішення цих питань на сьогодні значне поширення отримав контроль на основі ролей (RBAC), або ролевий доступ. Суть підходу полягає в створенні ролей, що повторюють бізнес-ролі на підприємстві, і присвоєння їх користувачам. На основі цих ролей перевіряється можливість виконання користувачем тієї або іншої дії.

Найчастіше ролевий доступ застосовується, якщо бізнес-роль є одновимірною і усі дії можна розбити по ролях (наприклад, бухгалтер, менеджер, адміністратор і т.ін.). Тоді однієї бізнес-ролі відповідатиме одна роль для контролю доступу (рис. 2.7).

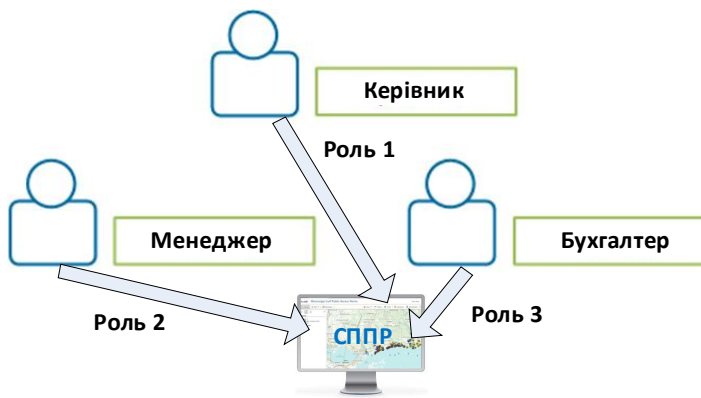


Рис. 2.7. Простий ролевий доступ

Але такий підхід не завжди дає ефективні результати. Бізнес-правила неминуче ускладнюються і стають багатовимірними. Наприклад, серед користувачів з'являється два бухгалтери, кілька менеджерів і т.д. Це призводить до того, що одного атрибуту (ролі) для відображення бізнес-правил стає недостатнім і починають додаватися інші атрибути (філія підприємства, день тижня, у який дозволено доступ, власник ресурсу, ліміт і т.ін.). Щоб впоратися з цією складністю, необхідно створювати додаткові ролі, число яких дорівнює числу різних комбінацій усіх атрибутів.

Окрім цього, з'являються й інші проблеми – одне бізнес-правило «розмазується» серед множини ролей і стає неочевидним, що ускладнює розуміння такого правила і його підтримку для контролю. Крім того, починається вибухове зростання кількості ролей, що значно ускладнює керування ними. Існують також бізнес-правила, в яких використовуються атрибути, значення яких заздалегідь не відомі і обчислюються в процесі роботи. Їх взагалі неможливо виразити за допомогою ролевої моделі. Також складно відобразити за допомогою ролевої моделі і бізнес-правила, які обмежують доступ не до дій (процедур), а до даних (об'єктів).

Щоб впоратися з нерозв'язними у рамках RBAC проблемами, був створений інший підхід, який ґрунтується на атрибутах – ABAC (Attribute – based access control). Основна відмінність цього підходу полягає у тому, що кожна ситуація оцінюється не з точки зору ролі користувача і дії, яку він хоче вчинити, а з точки зору атрибутів, які до них відносяться. Бізнес-правило, по суті, є набором умов, в яких різні атрибути повинні задовольняти вимогам, що пред'являються до них. Виділяються декілька категорій атрибутів, наприклад, як наведено на рис. 2.8.

Рис. 2.8. Атрибути бізнес-ролі

Для виконання авторизації значення усіх атрибутів беруться у момент перевірки прав і порівнюються з очікуваними значеннями. Виконання усіх умов забезпечує доступ до ресурсу. Таким чином, перевага ABAC, яка полягає у тому, що при додаванні нових значень атрибутів умови бізнес-правила змінюватися не будуть, дозволяє уникнути проблем, які з'явля-

ються при використанні RBAC. Крім того, на сьогодні для ABAC існує стандарт XACML, який активно розвивається і використовується.

Крім названих політик знайшли застосування й деякі менш універсальні політики.

Політика ізольованого програмною середовища визначає безпечний порядок взаємодії суб'єктів системи, який унеможливлює породження нових суб'єктів та їхній вплив на систему захисту через небезпечну модифікацію чи конфігурацію її параметрів. Відповідно до політики ізольованого програмного середовища вся множина інформаційних потоків у системі розподіляється на дві підмножини потоків, що не перетинаються – потоки несанкціонованого доступу і потоки легального доступу. Потоки несанкціонованого доступу підлягають фільтрації. Таке розподілення та фільтрацію має здійснювати певний суб'єкт, який дістав назву монітор безпеки об'єктів.

Політика безпеки інформаційних потоків визначає безпечний порядок взаємодії об'єктів у системі. Ця політика полягає у розподіленні множини інформаційних потоків у системі на дві підмножини потоків – бажаних і небажаних, що не перетинаються, і унеможливлює породження в системі небажаних інформаційних потоків.

2.4.3. Документування політики безпеки

Політика безпеки, як документ, може мати різний зміст у залежності від масштабів системи та її призначення. Це може бути директива керівника підприємства з організації кібербезпеки, що встановлює цілі і призначає відповідальних за її виконання. Або це може бути рішення начальника відділу, в якому експлуатується СППР, щодо безпеки електронної пошти. Це можуть бути й правила забезпечення безпеки конкретно для системи (це політики, котрі реалізуються передусім програмно-апаратними засобами.

У будь якому випадку необхідним елементом політики є ухвалення рішення у відношенні даного питання. Воно задає обґрунтований напрямок діяльності, вибраний із декількох можливих. Крім того, політика має інтегрувати усі питання, пов'язані з організацією інформаційної безпеки підприємства (рис. 2.9).

Для того щоб описати політику по даній області безпеки, адміністратори спочатку повинні визначити самому область за допомогою обмежень і умов у зрозумілих усім термінах, або ввести деякі з термінів та явно зазначити ціль або причини розробки політики. Як тільки предмет політики описаний, визначені основні поняття і розглянуті умови застосування політики, треба в явній формі описати позицію підприємства (тобто

рішення його керівництва) з даного питання. Це означає, що треба уточнити де, як, коли, ким і до чого застосовується дана політика. Потрібно описати відповідальних посадових осіб та їхні обов'язки у відношенні розробки і впровадження різноманітних аспектів політики.

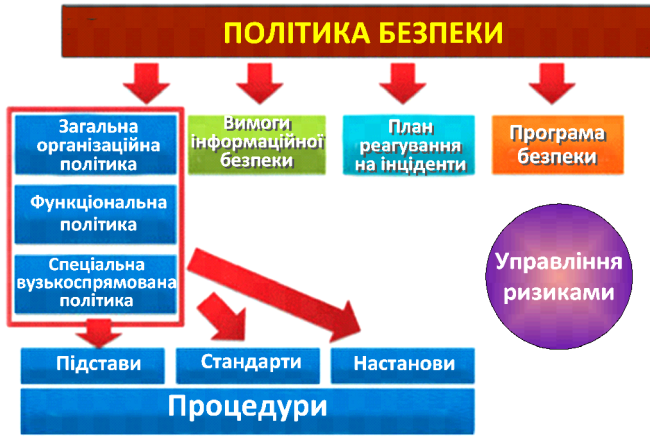


Рис. 2.9. Політика безпеки як засіб інтегрування питань забезпечення інформаційної безпеки

Для ефективності політика безпеки повинна бути наочною. Наочність допомагає реалізувати політику, допомагаючи гарантувати її знання і розуміння всіма співробітниками підприємства. Програма навчання в області кібербезпеки і контрольні перевірки дій у тих або інших ситуаціях можуть достатньо ефективно поінформувати всіх користувачів про політику. З нею також потрібно знайомити усіх нових працівників.

Для того щоб бути ефективної, політика повинна бути узгодженою з іншими існуючими директивами, законами, наказами і загальними задачами підприємства. Вона також повинна бути інтегрованою і узгодженою з іншими політиками (наприклад, політикою з приймання працівників на роботу).

Політику безпеки доцільно розглядати на трьох рівнях деталізації. До *верхнього рівня* можна віднести рішення, що стосуються підприємства в цілому. Вони носять досить загальний характер і, як правило, виходять від керівництва. Зразковий список подібних рішень може містити в собі наступні елементи:

- рішення сформувати або переглянути комплексну програму забезпечення безпеки, призначення відповідальних за просування програми;

- формулювання цілей, які переслідує підприємство в сфері кібербезпеки, визначення загальних напрямків у досягненні цих цілей;
- забезпечення бази для дотримання законів і правил;
- формулювання адміністративних рішень по тим питанням реалізації програми безпеки, які повинні розглядатися на рівні підприємства в цілому.

На верхній рівень виноситься управління захисними ресурсами й координація використання цих ресурсів, виділення спеціального персоналу для захисту критично важливих систем і взаємодія з іншими організаціями, що забезпечують або контролюють режим безпеки.

Політика верхнього рівня повинна чітко окреслювати сферу свого впливу. Можливо, це будуть всі автоматизовані системи підприємства (або навіть більше, якщо політика регламентує деякі аспекти використання співробітниками своїх домашніх комп'ютерів). Можлива, однак, і така ситуація, коли в сферу впливу включаються лише одна, найбільш важлива система.

Загалом кажучи, на верхній рівень варто виносити мінімум питань. Подібне винесення доцільне, коли воно обіцяє значну економію коштів або коли інакше зробити просто неможливо.

До *середнього рівня* можна віднести питання, що стосуються окремих аспектів кібербезпеки, але важливі для різних систем, що експлуатуються на підприємстві. Приклади таких питань – ставлення до передових технологій, доступ в Інтернет, використання домашніх комп'ютерів (віддалена робота), власних мобільних засобів (так званий *BYOD – Bring Your Own Device,* що перекладається як «принеси свій власний пристрій"), застосування користувачами неофіційного програмного забезпечення й т.ін. Також на цьому рівні має визначитись позиція підприємства та керівництва ІТ-підрозділу щодо застосування в системах вільного/відкритого програмного забезпечення.

Політика середнього рівня повинна висвітлювати такі теми, як область застосування, позиція підприємства по аспектам політики цього рівня, ролі й обов'язки користувачів, а також точки контакту, тобто має бути відомо, куди варто звертатися за роз'ясненнями, допомогою й додатковою інформацією щодо реалізації політики.

Політика безпеки нижнього рівня відноситься до конкретних інформаційних сервісів. Вона містить у собі два аспекти – цілі й правила їхнього досягнення, тому її часом важко відокремити від питань реалізації. На відміну від двох верхніх рівнів, розглянута політика повинна бути визначена більш докладно. Є багато речей, специфічних для окремих видів послуг, які не можна єдиним способом регламентувати навіть в рамках

однієї системи. У той же час, ці речі є настільки важливими для забезпечення режиму безпеки, що стосовно до них рішення повинні прийматися на управлінському, а не на технічному рівні. У політиці безпеки нижнього рівня варто висвітлити такі, наприклад, питання, як хто має право доступу до об'єктів, що підтримуються сервісом, при яких умовах можна читати й модифікувати дані, як організований віддалений доступ до сервісу і т.ін.

При формулюванні цілей політики нижнього рівня можна виходити з міркувань цілісності, доступності й конфіденційності, але не можна на цьому зупинятися. Її цілі повинні бути більш конкретними. Наприклад, якщо мова йде про систему підтримки прийняття рішень щодо стратегії заробітної плати на підприємстві, можна поставити мету, щоб тільки співробітникам відділу кадрів і бухгалтерії дозволялося вводити й модифікувати інформацію. У більш загальному випадку цілі повинні зв'язувати між собою об'єкти сервісу й дії з ними.

Із цілей виводяться правила безпеки, що описують, хто, що й при яких умовах може робити. Чим докладніше правила, чим більш формально вони викладені, тим простіше підтримати їхнє виконання програмно-технічними засобами. З іншого боку, занадто жорсткі правила можуть заважати роботі користувачів. Авторами політики має бути знайдений розумний компроміс, коли за прийнятну ціну буде забезпечений прийнятний рівень безпеки, а співробітники не виявляться надмірно навантажені.

У відношенні розробки і впровадження різних аспектів політики потрібно описати відповідальних посадових осіб і їхні обов'язки. Наприклад, для такого складного питання, як безпека в Internet, організації може знадобитися увести відповідальних за аналіз безпеки різних архітектур чи за затвердження використання тієї чи іншої архітектури.

Нарешті, у «політичний» документ необхідно включити інформацію про посадових осіб, що відповідають за проведення політики безпеки в життя. Мають бути перераховані групи людей, що відповідають за реалізацію сформульованих раніше цілей на своїх ділянках, такі як керівники підрозділів, адміністратори локальної мережі, адміністратори сервісів, користувачі, тощо.

Нижче наведено орієнтовний перелік окремих документів, що можуть складати документальний комплекс політики безпеки СППР, а саме:

1. Концепція забезпечення інформаційної безпеки в СППР;

2. План захисту від несанкціонованого доступу до інформації і незаконного втручання в процес функціонування СППР;

3. Положення про категорування ресурсів СППР;

4. Порядок поводження з інформацією, що підлягає захисту;

5. План забезпечення безупинної роботи і відновлення;
6. Обов'язки адміністратора інформаційної безпеки СППР;
8. Пам'ятка користувачу СППР щодо забезпечення безпеки;
9. Інструкція з внесення змін у списки користувачів СППР;
10. Інструкція з модифікації технічних і програмних засобів;
11. Інструкція з організації парольного захисту;
12. Інструкція з організації антивірусного захисту;

Також документально необхідно визначити відповідальність за реалізацію сформульованих цілей ПІБ, а саме:

- керівники підрозділів відповідають за доведення положень політики безпеки до користувачів і за контакти з ними;
- адміністратори програмно-технічних засобів (локальної мережі, серверів) забезпечують безупинне функціонування обладнання і відповідають за реалізацію технічних заходів, необхідних для проведення в життя політики безпеки;
- адміністратори сервісів відповідають за конкретні сервіси і, зокрема, за те, щоб захист був побудований відповідно до загальної політики безпеки;
- користувачі зобов'язані працювати з системою відповідно до політики безпеки, підкорятися розпорядженням осіб, що відповідають за окремі аспекти безпеки, доводити до відома керівництво про всі підозрілі ситуації.

2.4.4. Програма безпеки

Після того, як сформульована політика безпеки, приступають до складання програми її реалізації й власне до реалізації.

Щоб зрозуміти й реалізувати яку-небудь програму, її потрібно структурувати по рівнях, зазвичай у відповідності до структури підприємства або тих підрозділів, що використовують систему та її обслуговують. У найпростішому й найпоширенішому випадку достатньо двох рівнів – верхнього, або центрального, котрий охоплює усе підприємство, і нижнього, або службового, котрий відноситься до окремих послуг або груп однорідних сервісів.

Програму верхнього рівня очолює особа, відповідальна за інформаційну безпеку на підприємстві. У цієї програми мають бути відображені наступні головні цілі:

- управління ризиками (оцінка ризиків, вибір ефективних засобів захисту);
- координація діяльності в сфері кібербезпеки, поповнення й розподіл ресурсів;

- стратегічне планування;
- контроль діяльності в сфері кібербезпеки.

У рамках програми верхнього рівня приймаються стратегічні рішення щодо забезпечення безпеки, оцінювання технологічних новин, відстеження й впровадження нових засобів.

Контроль діяльності в галузі безпеки має двосторонню спрямованість. По-перше, необхідно гарантувати, що дії підприємства не суперечать законам. При цьому варто підтримувати контакти із зовнішніми контролюючими організаціями. По-друге, потрібно постійно відслідковувати стан безпеки усередині підприємства, реагувати на випадки порушень і допрацьовувати захисні заходи з урахуванням зміни обстановки.

Варто підкреслити, що програма верхнього рівня повинна займати строго чинне місце в діяльності підприємства, вона повинна офіційно прийматися та підтримуватися керівництвом, а також мати визначений штат і бюджет.

Мета програми нижнього рівня – забезпечити надійний і економічний захист конкретного сервісу або групи однорідних сервісів. На цьому рівні вирішується, які варто використовувати механізми захисту, закладаються питання закупівлі та встановлювання технічних та програмних засобів, передбачається адміністрування, відслідковування стану слабких місць у захисті і т.ін. Звичайно за програму нижнього рівня відповідають адміністратори систем і сервісів.

Головна вимога до програм безпеки – це їх синхронізація з життєвим циклом автоматизованих систем. Якщо синхронізувати програму безпеки нижнього рівня з життєвим циклом сервісу, що захищається, можна домогтися більшого ефекту з меншими витратами. Відомо, що додати нову можливість до вже готової системи значно складніше, ніж з самого початку спроектувати й реалізувати її. Те ж саме є слушним й для засобів захисту.

2.4.5. Управління ризиками

Використання СППР, як і більшості з інших автоматизованих систем, пов'язане з певною сукупністю ризиків, у тому числі й стосовно можливих збитків від порушень безпеки. Разом із тим інформаційна безпека повинна досягатися економічно виправданими заходами. Коли можливий збиток є занадто великим, необхідно прийняти відповідні заходи захисту, але вони мають бути економічно виправданими. Оцінюючи розмір збитку, необхідно мати на увазі не тільки безпосередні витрати на заміну обладнання або відновлення інформації, але й більш віддалені, такі як підрив репутації, ослаблення позицій на ринку й т.п. Таким чином необхідно виз-

начити рівень мінімальних затрат на безпеку, при якому досягається прийнятний рівень захищеності (рис. 2.10).

Тому управління ризиками розглядається на адміністративному рівні, оскільки тільки керівництво підприємства здатне виділити необхідні ресурси, ініціювати й контролювати виконання відповідних програм. також для контролю ефективності діяльності в сфері безпеки та для урахування змін обстановки необхідна періодична оцінка ризиків.

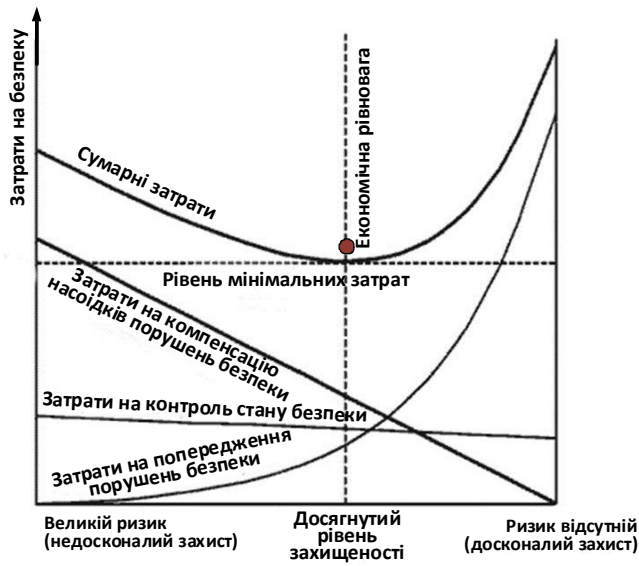


Рис. 2.10. Співвідношення затрат на забезпечення інформаційної безпеки та досягнутим рівнем захищеності

З кількісної точки зору рівень ризику є функцією ймовірності реалізації певної загрози (що використовує деякі уразливі місця), а також розміри можливого збитку, критичного для цінних активів підприємства (рис. 2.11). Таким чином, суть заходів щодо управління ризиками полягає в тому, щоб оцінити їхній розмір, виробити ефективні й економічні заходи зниження ризиків, а потім переконатися, що ризики укладені в прийнятні рамки (і залишаються такими).

Ризики потрібно контролювати постійно, періодично проводячи їхню переоцінку, тобто управління ризиками є процесом циклічним, що базується на відомій дефініції Plan-Do-Chek-Act, що означає «плануй-виконуй-перевіряй-вдосконалюй» (рис. 2.12).

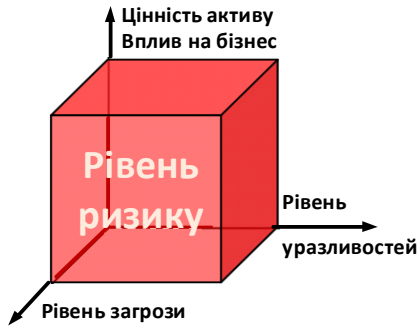


Рис. 2.11. Визначення рівня ризику

Отже, управління ризиками містить у собі наступні етапи:

1. Вибір об'єктів для аналізу і рівня деталізації їхнього розгляду.
2. Вибір методології оцінки ризиків.
3. Ідентифікація активів.
4. Аналіз загроз і їхніх наслідків, виявлення уразливих місць у захисті.
5. Оцінка ризиків.
6. Вибір захисних заходів.
7. Реалізація (впровадження) обраних заходів.
8. Перевірка результативності обраних заходів (моніторинг заходів).
9. Оцінка залишкового ризику.

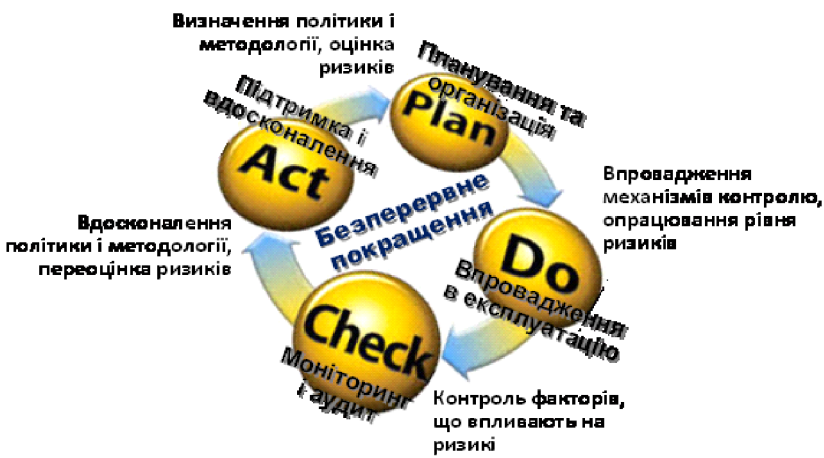


Рис. 2.12. Циклічний процес управління ризиками

Стосовно виявлених ризиків можливі наступні дії:

- ліквідація ризику (наприклад, за рахунок усунення причини);
- зменшення ризику (наприклад, за рахунок використання додаткових захисних засобів);
- прийняття ризику (і вироблення плану дії у відповідних умовах);
- переадресація ризику (наприклад, шляхом укладання страхової угоди).

Коли передбачені заходи будуть упроваджені, необхідно перевірити їхню дієвість, тобто переконатися, що залишкові ризики стали прийнятними. Якщо це насправді так – можна намічати дату наступної переоцінки. У протилежному випадку доведеться проаналізувати допущені помилки й невідкладно провести повторний сеанс управління ризиками.

2.4.6. Підтримка працездатності та реагування на порушення режиму безпеки

Підтримка працездатності СППР включає низку рутинних заходів, тому саме тут ховається найбільша небезпека. Ненавмисні помилки системних адміністраторів і користувачів загрожують ушкодженням обладнання, руйнуванням програм і даних, також створюють проломи в захисті, які уможливлюють реалізацію загроз.

Можна виділити наступні напрямки повсякденної діяльності з підтримки працездатності:

- підтримка користувачів;
- підтримка програмного забезпечення;
- конфігураційне керування;
- резервне копіювання;
- керування носіями;
- документування;
- регламентні роботи.

Підтримка користувачів має на увазі насамперед консультування й надання допомоги при вирішенні різного роду проблем. Зазвичай цим займається системний адміністратор, але доцільніше цей процес автоматизувати, створивши для цієї мети спеціальну систему «довідковий стіл» (help desk), що значно покращує ефективність допомоги користувачам (рис. 2.13).

Одним з найважливіших заходів забезпечення цілісності інформації є підтримка програмного забезпечення, яка передбачає стеження за тим, яке програмне забезпечення встановлене на комп'ютерах користувачів, а також за неавторизованими змінами програм і прав доступу до них. До цього ж можна віднести підтримку еталонних копій програмних систем.

Зазвичай контроль досягається комбінуванням засобів фізичного й логічного керування доступом, а також використанням утиліт перевірки й забезпечення цілісності.

Рис. 2.13. Процес підтримки користувачів з використанням системи «довідковий стіл»

Конфігураційне керування спрямоване на контроль і фіксування змін, внесених в програмну конфігурацію системи. Це дозволяє застрахуватися від випадкових або непродуманих модифікацій, забезпечити повернення (відкат) до попередньої, працюючої, версії. Кращий спосіб зменшити кількість помилок у цій рутинній роботі – максимально автоматизувати її.

Для відновлення програм і даних після аварій перевіреним засобом є резервне копіювання. Тут також доцільно автоматизувати роботу, сформувавши комп'ютерний розклад створення повних і інкрементальних копій, а також використовувати відповідні програмні продукти.

Для забезпечення фізичного захисту й обліку змінних носіїв інформації («флешек», знімних жорстких дисків, роздруківок) необхідно керувати носіями. Воно має забезпечувати конфіденційність, цілісність і доступність інформації, що зберігається поза комп'ютерними системами. Під захистом тут розуміється не тільки відвертання несанкціонованого доступу, але й запобігання шкідливих впливів навколишнього середовища (спеки, холоду, вологи, магнетизму, тощо).

Невід'ємною частиною забезпечення інформаційної безпеки є документування. У вигляді документів оформлюється майже все – від політики безпеки до журналу обліку носіїв. Важливо, щоб документація була актуальної, відображала поточний стан справ, причому в несуперечливому виді, і надійно зберігалася.

Дуже серйозною загрозою безпеки є регламентні роботи. Співробітник, що здійснює регламентні роботи, отримує доступ до системи з ви-

нятковими правами, і на практиці дуже важко проконтролювати, які саме дії він втілює. Тому на перший план виходить ступінь довіри до тих, хто виконує робот, і їх ретельний добір.

На жаль, незважаючи на вжиті заходи з безпеки, порушникам вдається скористатися проломами у захисті та завдати шкоди системі. Що ж робити у випадку порушень режиму безпеки? Насамперед, набір оперативних заходів, спрямованих на виявлення й нейтралізацію порушень режиму безпеки повинна передбачати програма безпеки. Важливо, щоб послідовність дій у подібних випадках була спланованою заздалегідь, оскільки заходи з відновлення потрібно приймати термінові й скоординовані.

Реакція на порушення режиму безпеки переслідує три головні цілі:

- локалізація інциденту й зменшення задіяної шкоди;
- виявлення порушника;
- попередження повторних порушень.

На підприємстві має бути служба (окрема людина), що є доступною 24 години на добу (особисто, по телефону, електронною поштою), яка відповідає за реакцію на порушення. Усі повинні знати координати відповідальної людини й звертатися до неї при перших ознаках небезпеки. Потрібно знати також що робити до появи фахівця на місті події.

Як показує практика, виявити порушника дуже складно, тому потрібно заздалегідь підготувати і мати під рукою контактні координати можливих помічників у цій справі – постачальника мережних послуг, служби охорони, тощо, та мати домовленість з ним про можливість і порядок виконання відповідних дій. Нарешті, щоб запобігти повторним порушенням, необхідно аналізувати кожний інцидент, виявляти причини, відслідковувати появу нових уразливих місць, якнайшвидше ліквідувати асоційовані з ними вікна небезпеки, а також накопичувати статистику порушень.

Підготуватися до можливих аварій, зменшити збиток від них і зберегти здатність до функціонування системи хоча б у мінімальному обсязі дозволяє *планування відбудовних робіт*. Процес планування відбудовних робіт можна розділити на наступні етапи:

- виявлення критично важливих функцій системи, встановлення пріоритетів;
- ідентифікація ресурсів, необхідних для виконання критично важливих функцій;
- визначення переліку можливих аварій;
- розробка стратегії відбудовних робіт;
- підготовка до реалізації обраної стратегії;
- перевірка стратегії.

Плануючи відбудовні роботи, варто усвідомлювати те, що повністю зберегти функціонування системи не завжди можливо. Необхідно виявити критично важливі функції, без яких функціонування системи не має сенсу, і навіть серед критичних функцій розставити пріоритети, щоб якнайшвидше й з мінімальними витратами відновити роботу після аварії.

Ідентифікуючи ресурси, необхідні для виконання критично важливих функцій, бажано підключати до роботи фахівців різного профілю, здатних у сукупності охопити всі аспекти проблеми. Критичні ресурси звичайно відносяться до однієї з наступних категорій: 1) персонал; 2) інформаційна інфраструктура; 3) фізична інфраструктура.

При визначенні переліку можливих аварій потрібно спробувати розробити їхні сценарії, передбачивши відповіді на такі питання, як будуть розвиватися події, які можуть виявитися масштаби наслідків, що відбудеться із критичними ресурсами та т.ін.

Стратегія відбудовних робіт повинна базуватися на наявних ресурсах і бути не занадто накладною для підприємства. При розробці стратегії доцільно провести аналіз ризиків, яким піддаються критичні функції, і вибрати найбільш економічне рішення. Стратегія повинна передбачати не тільки роботу за тимчасовою схемою, але й повернення до нормального функціонування. Підготовка до реалізації обраної стратегії складається у виробленні плану дій в екстрених ситуаціях і по їх закінченні. Має сенс також укласти додаткову угоду з розробником системи про першочергове обслуговування в критичних ситуаціях.

2.4.7. Управління персоналом

Вже неодноразово зверталася увага на важливість так званого «людського фактору» при розгляді питань безпеки. Тому керування персоналом відноситься до адміністративного рівня і має бути відображеним у політиці безпеки.

Управління персоналом починається із прийому нового співробітника на роботу й навіть раніше – зі складання опису посади (посадової інструкції). Уже на даному етапі бажано підключити до роботи фахівця з інформаційної безпеки – не лише для того, щоб випадково не прийняти на роботу людину з карним минулим або психічним захворюванням, але й для визначення особливостей майбутньої роботи співробітника як користувача СППР, що асоційовані з його посадою. Існує два загальних принципи, які варто мати на увазі – *розділення обов'язків* та *мінімізація привілеїв*.

Принцип розділення обов'язків приписує так розподіляти ролі й відповідальність, щоб одна людина не могла порушити критично важливий для

системи процес. При цьому важливо передбачити процедурні обмеження дій суперкористувача. Можна штучно «розщепити» пароль суперкористувача, повідомивши першу його частину одному співробітникові, а другу – іншому. Тоді критично важливі дії, наприклад, з адміністрування системи., вони зможуть виконати тільки вдвох, що знижує ймовірність помилок і зловживань.

Принцип мінімізації привілеїв пропонує виділяти користувачам тільки ті права доступу, які необхідні їм для виконання службових обов'язків. Призначення цього принципу є очевидним – зменшити збиток від випадкових або навмисних некоректних дій.

Коли кандидат визначений, він повинен пройти навчання. Його варто докладно ознайомити не лише зі службовими обов'язками, з й з порядком роботи з системо, а також з нормами й процедурами інформаційної безпеки. Бажано, щоб заходи безпеки були ним засвоєні до вступу на посаду й до заведення його системного рахунку із логіном, паролем і привілеями.

З моменту заведення системного рахунку починається його адміністрування, а також протоколювання й аналіз дій користувача. Поступово змінюється оточення, у якому працює користувач, його службові обов'язки і т.ін. Все це вимагає відповідної зміни привілеїв. Технічну складність викликають тимчасові переміщення користувача, виконання ним обов'язків замість співробітника, що пішов у відпустку, інші обставини, коли повноваження потрібно спочатку надати, а через якийсь час позбавити них. У такі періоди профіль активності користувача різко змінюється, що створює труднощі при виявленні підозрілих ситуацій. Певної акуратність варто дотримуватись й при видачі нових постійних повноважень, не забуваючи ліквідувати старі права доступу.

У випадку конфлікту між співробітником і підприємством можливе фізичне обмеження доступу до автоматизованого робочого місця або блокування системного рахунку. Якщо співробітник звільняється, має проводитися максимально оперативно ліквідація системного рахунку користувача, у нього потрібно не лише прийняти все його комп'ютерне господарство, а й зокрема криптографічні ключі, якщо використалися засоби шифрування або електронного цифрового підпису.

До керування співробітниками примикає адміністрування осіб, що працюють за контрактом (наприклад, фахівців фірми-постачальника системи). Відповідно до принципу мінімізації привілеїв, їм потрібно виділити рівно стільки прав, скільки необхідно, і вилучити ці права відразу по закінченні контракту.

Для забезпечення ефективності управління персоналом вищеназвані процеси бажано автоматизувати. Особливо це важливо на підприємстві з територіально-розподіленою структурою.

Контрольні запитання та завдання

1. У чому полягає головна мета заходів адміністративного рівня?
2. Поясніть кроки, з яких зазвичай складається процес створення політики безпеки.
3. Що слід розуміти під політикою безпеки на адміністративному рівні?
4. Роз'ясніть сутність ролевої політики доступу, її переваги та недоліки.
5. Приведіть особливості документування політики безпеки на підприємстві.
6. Чому управління ризиками розглядається на адміністративному рівні?
7. Обрисуйте загальну схему управління ризиками та її особливості.
8. Назвіть напрямки повсякденної діяльності з підтримки працездатності.
9. У чому полягають заходи з підтримки користувачів?
10. Поясніть два загальних принципи управління персоналом, що користується СППР та обслуговує її.

3. ПРОГРАМНО-ТЕХНІЧНІ ЗАСОБИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ СППР

3.1. ОСНОВНІ ТЕХНОЛОГІЇ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ СППР

Класифікація засобів забезпечення інформаційної безпеки.

Питання забезпечення кібербезпеки СППР, як витікає з попередніх розділів, у загальному уявленні фактично зводиться до запобігання *НСД – несанкціонованого доступу (unauthorized access to information)* до інформації і до сервісів системи. Згідно з даними щорічних оглядів комп'ютерної злочинності, що проводяться різними поважними міжнародними агенціями, майже постійно на перших місцях за розміром збитку підприємств знаходяться несанкціонований (неавторизований) доступ і крадіжка конфіденційних даних.

НСД є навмисним зверненням користувача до даних, доступ до яких йому не дозволений, з метою їхнього читання, відновлення або руйнування, та може бути здійснений людиною або ініційованою їм програмою стосовно інформації, що захищається, а також людиною стосовно штатних засобів системи, що захищаються. Несанкціонований доступ може створити будь-яку з загроз безпеки інформації: витік, розсекречення, порушення цілісності або доступності (блокування).

У широкому сенсі захист інформації від НСД – це діяльність, спрямована на запобігання одержання інформації, що захищається, зацікавленим суб'єктом з порушенням прав або правил доступу до інформації, встановлених правовими документами або власником, володільцем інформації.

НСД реалізується з застосуванням таких основних способів, як безпосереднє звернення до об'єктів доступу, створення програмних і технічних засобів, що виконують звернення до об'єктів доступу в обхід засобів захисту, модифікація засобів захисту, що дозволяє здійснити НСД, впровадження в технічні засоби АІС програмних або технічних механізмів, що

порушують передбачувану структуру й функції АІС і що дозволяють здійснити НСД. Способи і методи НСД, як правило, використовуються комплексно, створюючи так звані сценарії НСД.

Одними з основних перевірених шляхів захисту від НСД є забезпечення захисту комплексом програмно-технічних засобів, що реалізують певні захисні технології. Які ж основні технології мають застосовуватись в СППР для забезпечення кібербезпеки, у тому числі й захисту від НСД?

На основі досвіду створення і застосування комплексу засобі захисту в автоматизованих системах у вигляді програмно-технічних засобів (апаратної і програмної складових), які відповідають вимогам довірчої комп'ютерної бази (ТСВ), типову структуру комплексу засобів захисту в СППР можна представити як на рис. 3.1.

Рис. 3.1. Типова структура комплексу засобів захисту в СППР

Цей комплекс доцільно будувати у вигляді взаємозалежних підсистем, які утворюють систему захисту інформації (СЗІ). Побудова СЗІ в такому виді дозволяє забезпечити комплексність захисту інформації в СППР, керованість процесу і можливість адаптації при зміні умов функціонування СППР.

Виходячи з цього СЗІ має складатися з таких підсистем:

- ідентифікації й автентифікації;
- контролю доступу;
- протоколювання та аудиту;
- криптографічного захисту;
- забезпечення цілісності електронних документів з застосуванням електронного цифрового підпису (ЕЦП);

- мережевої безпеки;
- антивірусного захисту.

Також має бути передбачено засоби захисту в операційній системі, забезпечення високої доступності, аналіз захищеності та управління (менеджмент) безпекою.

Розгляду наведених засобів буде присвячено наступні параграфи посібника, а зараз лише коротко познайомимося з цими технологіями.

Захист інформації в СППР від несанкціонованого доступу в основному забезпечується технологіями *автентифікації* та *ідентифікації*, які підтримують процес перевірки достовірності наданої користувачем інформації про себе при вході у систему. Контроль прав доступу користувача ґрунтується на перевірці імені користувача, під яким він зареєстрований в системі, його паролю, а також на обмеженнях облікового запису та обмеженнях в часі. Автентифікація персоналу, зокрема з використанням біометричних систем, також займає важливе місце й у захисті підтримуючої інфраструктури (наприклад, приміщення центру обробки даних).

Засоби *керування доступом* традиційно дозволяють специфікувати і контролювати дії, які суб'єкти (користувачі й процеси) можуть виконувати над об'єктами (інформацією й іншими комп'ютерними ресурсами) після того, як вони отримали дозвіл після проведення процедур ідентифікації і автентифікації.

Одним з найважливіших напрямів діяльності у сфері забезпечення безпеки інформації був і залишається захист інформації шляхом шифрування, тобто *криптографічними* методами. Важливість цієї технології підкреслює відомий вислів, що «велика держава – це країна, що володіє ядерними технологіями, ракетною технікою і криптографією».

Автентифікація *(Authentication)* – Система перевірки прав користувача, призначена забезпечити безпеку роботи в АІС (зокрема, в мережі).

Ідентифікація *(Authentication)* – Система перевірки прав користувача, призначена забезпечити безпеку роботи в АІС (зокрема, в мережі).

Криптографічні методи дозволяють надійно *контролювати цілісність* як окремих порцій даних, так і їхніх наборів (таких як потік повідомлень, документ), визначати автентичність джерела даних; гарантувати неможливість відмовитися від зроблених дій («неспростовність»). В основі криптографічного контролю цілісності лежить два поняття – хеш-функція та електронний цифровий підпис (ЕЦП).

Криптографія (від грецького *kryptos* – прихований і *graphein* – писати) – наука про математичні методи забезпечення конфіденційності (неможливості прочитання інформації сторонніми особами) і автентичності (цілісності і справжності авторства) інформації.

Сучасні СППР зазвичай використовують мережеві з'єднання, зокрема Інтернет. Фундаментальна проблема полягає в тому, що Інтернет при проектуванні не замислювалася як захищена мережа і побудований на уразливому стеку протоколів TCP/IP. Боротися з загрозами, властивими мережному середовищу, допомагають технології мережевої безпеки, зокрема засоби екранування мереж.

Безпека мережі *(Network security)* – заходи, які захищають інформаційну мережу від несанкціонованого доступу, випадкового або навмисного втручання в нормальні дії або намагань руйнування її компонентів.

Враховуючи значне поширення в наш час зловредних програм широкого застосування в автоматизованих системах знайшло *антивірусне програмне забезпечення* (АВПЗ), яке намагаються знайти, запобігти розмноженню і видалити комп'ютерні віруси та інші шкідливі програми, впроваджених у файли та пам'ять системи.

Оскільки повністю виключити можливість відмови або некоректної роботи системи, зокрема з-за реалізації атак, неможливо, рішення полягає у тому, щоб виявляти проблеми на найбільш ранніх стадіях, і одержувати про них найбільш докладну інформацію. Для цього, як правило, застосовується різне *ПЗ моніторингу та засоби протоколювання і аудиту системи,* які фіксують усі порушення та дозволяють вчасно сповіщати технічних фахівців про виявлені проблеми.

Серед загроз автоматизованим системам вагоме місце займають загрози, спрямовані безпосередньо на *операційній системі* персональних комп'ютерів та серверів. Тому у сучасних ОС передбачені певні засоби захисту, які потрібно вміло налаштовувати та ефективно використовувати. Доповнюють ці засоби організаційні заходи щодо поводження з операційними системами та програмним забезпеченням. Зазвичай перевага віддається застосуванню ОС, що вільно розповсюджуються (наприклад. з сімейства Linux), особливо що стосується мережних серверів.

Автоматизована система надає своїм користувачам певний набір послуг (сервісів). Говорять, що забезпечено потрібний рівень доступності

цих сервісів, якщо визначені показники знаходяться у заданих межах. Тому комплекс *забезпечення високої доступності* та аналіз захищеності системи є невід'ємними складовими комплексу засобів безпеки. Сервіс *аналізу захищеності* призначений для виявлення уразливих місць з метою їхньої оперативної ліквідації.

Складність сучасних СППР є такою, що без правильно організованого керування вони поступово деградують не лише у плані функціональної ефективності, а й в плані захищеності. Дії з керування, що забезпечують нормальну роботу компонентів і засобів безпеки, відносяться до *поняття управління,* або *менеджменту інформаційної безпеки.*

Менеджмент інформаційної безпеки *(information security management)* – у загальному визначенні це управління ключовими структурами усіх підсистем і забезпечення їх взаємодії з метою постійного поліпшення рівня безпеки.

Контрольні запитання та завдання

1. У чому полягає основний перевірений шлях захисту від НСД?
2. Представте типову структуру комплексу програмно-техніч-них засобів захисту в СППР.
3. Які технології дозволяють боротися з загрозами, властивими мережному середовищу?
4. Для чого в СППР застосовують ПЗ моніторингу та засоби протоколювання і аудиту?
5. Приведіть особливості СППР, що вимагають застосування методів менеджменту інформаційної безпеки.

3.2. ІДЕНТИФІКАЦІЯ Й АВТЕНТИФІКАЦІЯ, КЕРУВАННЯ ДОСТУПОМ

Класифікація технологій ідентифікації/автентифікації. Парольна автентифікація. Технології ідентифікації. Керування доступом

3.2.1. Загальні положення

Важливим елементом політики безпеки як набору правил розмежування доступу є *механізм підзвітності*. Ціль підзвітності – у кожний момент часу знати, хто працює в системі й що робить. Засоби підзвітності поділяються на три категорії:

- ідентифікація й автентифікація;
- надання довіреного шляху;
- аналіз реєстраційної інформації.

Звичайний спосіб *ідентифікації* – уведення імені користувача при вході в систему. Стандартний засіб *перевірки дійсності (автентифікації)* користувачів – пароль.

Довірений шлях зв'язує користувача безпосередньо з довіреною обчислювальною базою, минаючи інші, потенційно небезпечні компоненти АС.

Ціль надання довіреного шляху – дати користувачеві можливості переконатися в автентичності обслуговуючої його системи.

Аналіз реєстраційної інформації (аудит) має справу з діями (подіями), що так чи інакше зачіпають безпеку системи. Засоби аудиту розглянемо у подальших параграфах.

Отже, у захищеній системі використання сервісів розраховано на обслуговування іменованих (легальних) суб'єктів, тому ідентифікацію й автентифікацію можна вважати основою програмно-технічних засобів безпеки. Ідентифікація й автентифікація (ІдА) – це перша лінія оборони, «прохідна» інформаційного простору системи, основний засіб запобігання НСД.

Ідентифікація дозволяє суб'єктові (користувачу, процесу, що діє від імені певного користувача, або іншому апаратно-програмному компоненту) назвати себе (повідомити своє ім'я). За допомогою автентифікації друга сторона (система) переконується, що суб'єкт дійсно той, за кого він себе видає. Як синонім терміну «автентифікація» іноді використовують словосполучення «перевірка автентичності».

Для ідентифікації користувач уводить так званий логін (login), що зазвичай є його «ім'ям» – фактичним, наприклад, прізвище або ім'ям за паспортними даними, або умовний, вигаданий набір символів, який ототожнюється з даним користувачем. «Ім'я» є відомим системному адміністратору (адміністратору безпеки), а використання імен регламентується політикою безпеки.

Для підтвердження своєї автентичності суб'єкт, що намагається отримати доступ, може пред'явити, принаймні, одну з наступних сутностей:

- дещо, що відоме лише одному йому (пароль, особистий ідентифікаційний номер, криптографічний ключ і т.п.);
- дещо, чим лише він володіє (особисту картку або пристрій аналогічного призначення);
- дещо, що є частиною його самого (голос, відбитки пальців і т.ін., тобто свої біометричні характеристики).

Автентифікація буває однобічною – зазвичай суб'єкт (клієнт) доводить свою автентичність серверу, і двосторонньою (взаємною). Процедура входу користувача в систему є прикладом однобічної автентифікації.

Надійна ІдА утруднена з цілої низки причин. По-перше, майже всі автентифікаційні сутності можна дізнатися, поцупити або підробити. По-друге, є протиріччя між надійністю автентифікації, з одного боку, і зручностями користувача й системного адміністратора з іншого. Так, з міркувань безпеки необхідно з певною частотою змінювати автентифікаційну інформацію, а також вимагати від користувача періодичного повторного її введення, що зазвичай є клопітно. По-третє, чим надійніше засіб захисту, тим він дорожчий.

У відкритому мережному середовищі існують додаткові проблеми, адже між сторонами ІдА не існує довіреного маршруту; це означає, що в загальному випадку дані, передані суб'єктом, можуть не збігатися з даними, отриманими для перевірки автентичності. Необхідно забезпечити захист від пасивного й активного прослуховування мережі, тобто від перехоплення, зміни й/або відтворення даних. Передача паролів у відкритому виді є ризиковою; не рятує становища й шифрування паролів, тому що воно не захищає від відтворення. Тому потрібні більш складні протоколи автентифікації.

Таким чином, зазвичай необхідно шукати компроміс між надійністю, доступністю за ціною й зручністю використання й адміністрування засобів ІдА.

В останні роки інтенсивно розвивається напрямок електронної ІдА, у якій збір інформації відбувається з максимальною автоматичністю, тобто з мінімальною участю людини. Користувач може припуститися помилки при

уведенні даних, наприклад, із клавіатури комп'ютера, а технології автоматичної ІдА найбільше повно відповідають вимогам СППР, де потрібно чітко розпізнавати суб'єкти, найчастіше в реальному масштабі часу. Основна класифікація технологій ідентифікації й автентифікації наведена на рис. 3.2.

Рис. 3.2. Технології ідентифікації та автентифікації

Необхідно зазначити. що цю класифікацію можна вважати умовною, адже на практиці часто вказані технології використовуються в різних комбінаціях і виконують як ідентифікаційні, так і автентифікаційні завдання.

3.2.2. Парольна автентифікація

Головна перевага парольної автентифікації – простота й звичність. Паролі давно убудовані в операційні системи й інші сервіси. При правильному використанні паролі можуть забезпечити прийнятний рівень безпеки.

Технологічно це відбувається у наступному порядку. Служба автентифікації у системі містить у собі облікові записи користувачів, що зберігає ідентифікатор (login) і пароль (password) користувача у своїй базі даних. При спробі входу в систему користувач набирає свій пароль, що надходить у службу автентифікації. За підсумками порівняння пари login/password з еталонним значенням з бази даних облікових записів користувачів користувач може успішно пройти процедуру цієї найпростішої автентифікації й авторизуватися в системі.

Проте, за сукупністю характеристик парольну автентифікацію варто визнати найслабкішим засобом перевірки автентичності.

Щоб пароль було легко запам'ятовувати для багаторазового використання, його найчастіше вибирають простим (ім'я подруги, назва спортивної команди й т.п.). Однак простий пароль неважко вгадати, особливо якщо знати пристрасті даного користувача. За даними багатьох аналітичних компаній найчастіше користувачі використовують у якості пароля такі вирази, як password, 123456, qwerty, 111111 та подібне. Аналіз зломів

паролів свідчить, що найчастіше вони відбуваються саме на таких паролях.

Використання багаторазового пароля є ризиковим. Уведення пароля можна підглянути або вгадати, якщо неодноразово спостерігати за рухом пальців на клавіатурі. Не кажучи вже про звичку багатьох користувачів записувати паролі на клаптиках паперу і тримати їх поряд з комп'ютером.

Пароль можна вгадати «методом грубої сили», використовуючи, скажемо, словник, або просто перебором різних варіантів. В Інтернеті існують «облікові звалища» (credential dumps) – списки з логінів і паролів користувачів, які зловмисники можуть використовувати для добору паролів. Джерелом поповнення таких звалищ є витоки з різних систем. Так наприклад 2014 року з'явились повідомлення про виток в Інтернет бази даних з логінами і паролями користувачів Gmail, Mail.ru та Яндекса.

Якщо файл паролів зашифрований, але доступний для читання, його можна скачати до себе на комп'ютер і спробувати підібрати пароль, запрограмувавши повний перебір (передбачається, що алгоритм шифрування відомий). У вільному доступі з'явилась програма ocl-Hashcat-plus, яка може розшифровувати 55-символьні паролі. Програма використовує декілька методів перебору символів залежно від хеш-функції кодування. Програма може проводити вісім мільярдів порівнянь символів в секунду залежно від використовуваної хеш-функції.

Щоб підвищити надійність парольного захисту треба застосувати апробовані заходи, а саме:

- накладання технічних обмежень (пароль повинен бути не занадто коротким, він повинен містити літери, цифри, знаки пунктуації, враховувати регістр й т.п.);
- керування терміном дії паролів, їхня періодична зміна;
- обмеження доступу до файлу паролів;
- обмеження кількості невдалих спроб входу в систему (це утруднить застосування «методу грубої сили»);
- навчання користувачів особливостям використання паролів;
- використання програмних генераторів паролів (така програма, ґрунтуючись на нескладних правилах, може породжувати тільки благозвучні й, отже, такі паролі, що запам'ятовуються).

Набагато більш потужним і стійким до загроз засобом, особливо в мережному середовищі, є одноразові паролі (OTP – One Time Password). Суть концепції одноразових паролів полягає у використанні різних паролів при кожному новому запиті на надання доступу. Одноразовий пароль дійсний тільки для одного входу в систему. Технологія OTP заснована на

використанні двофакторних схем автентифікації й може бути класифікованою як посилена технологія автентифікації.

Однак використання OTP передбачає суттєве ускладнення відповідних засобів користувача і системи та передбачає використання серверу автентифікації, якому повинен бути відомий алгоритм генерації паролів і асоційовані з ним параметри; крім того, годинники клієнта й сервера повинні бути синхронізованими на основі системи єдиного часу.

Найпоширеніші апаратні реалізації одноразових паролів для користувачів мають назву OTP-токени. Вони мають невеликий розмір і випускаються у вигляді різних форм-факторах – брелока, смарт-карти, пристрою, комбінованого з USB-ключем. Однією з розповсюджених апаратних реалізацій одноразових паролів є технологія SecurID, що пропонується компанією RSA Security. Вона заснована на спеціальних калькуляторах – токенах, які щохвилини генерують новий код. Існують апаратні реалізації й інших алгоритмів генерації одноразових паролів. Наприклад, можна генерувати пароль по події – натисканню клавіші на пристрої. Таке рішення пропонує компанія Secure Computing у вигляді продукту Safeword. Апаратну реалізацію технології «запит-відповідь» постачає корпорація CryptoCard. Є навіть універсальні апаратні реалізації, які дозволяють перепрограмувати токени.

Якщо ж система функціонує у розподіленому мережному середовищі, у вузлах якого зосереджені суб'єкти – користувачі, а також клієнтські й серверні програмні системи, виникає додаткова проблема попарної автентифікації. Для її вирішення використовується централізоване зберігання автентифікаційних даних і застосування механізмів Single Sign-On (можливість одноразової автентифікації в кількох додатках). Прикладом такої реалізації є протокол Kerberos. який пропонує механізм взаємної автентифікації клієнта й сервера перед встановленням зв'язку між ними. Система Kerberos являє собою *довірену третю сторону* (тобто сторону, який довіряють усі), яка володіє секретними ключами суб'єктів, що обслуговуються, і такою, що допомагає їм у попарній перевірці автентичності.

Чимало компаній пропонують власні рішення щодо автентифікації. Так, компанія IBM поставляє продукт Tivoli Identity Manager, де оптимізовано систему ідентифікації особистості, яка дозволяє ефективно адмініструвати облікові записи і паролі для співробітників і зовнішніх користувачів.

Програмна платформа Entrust IdentityGuard компанії Entrust реалізує різноманітні методи строгої автентифікації користувачів. Ця платформа є універсальною з широким набором можливостей для багатофакторної автентифікації як різних груп користувачів, так і окремих внутрішніх і

зовнішніх користувачів. Платформа включає функціональні можливості для використання в корпоративному IT-середовищі, що дозволяє ввести нові фактори автентифікації для особливо уразливих ресурсів, що використовуються в режимі видаленого доступу на основі протоколів IP-SEC, SSL, Outlook Web Access і т.ін.

3.2.3. Технології ідентифікації

Як вказувалося, «електронізація» ідентифікації, у якій уведення ідентифікаційних даних відбувається з мінімальною участю людини, вирішує проблеми, пов'язані з «людським фактором". Якщо уведення пароля наражається на небезпеки, то що вже казати про логін, який зазвичай є відомим не лише користувачу.

Однією з найпоширеніших є технологія ідентифікації на основі карток із магнітною смугою. Такі картки вже тривалий час використовуються в системах контролю фізичного доступу (наприклад, на прохідних, для входу у приміщення з обмеженим доступом, тощо). Магнітні картки спрацьовують при проведенні в певному напрямку й з певною швидкістю по щілині рідера (зчитувателя). З метою схоронності інформації від випадкового розмагнічування магнітні смуги виготовлені з матеріалів, що вимагають сильних магнітних полів для запису й знищення інформації. Істотною перевагою магнітних карт є їхня низька вартість. До основних недоліків даної технології можна віднести обмеження по обсягу інформації, що може бути записаною на магнітну смугу, незахищеність від копіювання, а також чутливість до забруднення, механічних ушкоджень (наприклад, подряпин, зломам), впливу вологи, що скорочує термін служби картки.

Останнім часом знайшли застосування смарт-картки – пластикові картки стандартного розміру, що мають убудовану мікросхему. Для використання смарт-карт у комп'ютерних системах необхідний пристрій читання смарт-карт. Більшість подібних кінцевих пристроїв, або пристроїв з'єднання (IFD), здатні як зчитувати, так і записувати інформацію, якщо дозволяють можливості смарт-карти й права доступу. Пристрої читання смарт-карт можуть підключатися до комп'ютера за допомогою послідовного порту, слота PCMCIA або USB. Пристрій читання смарт-карт також може бути убудований в клавіатуру. Як правило, для доступу до захищеної інформації, що зберігається в пам'яті смарт-карти, потрібен пароль, називаний PIN-кодом.

Застосування смарт-карток дозволяє проводити не лише ідентифікацію, а й автентифікацію користувача. Таку ж роль виконують і USB-ключі, які є більш привабливими, оскільки USB став стандартним портом для

підключення периферійних пристроїв і тому не потрібно купувати для користувачів які б то не було зчитувателі.

Мікропроцесорні смарт-картки й USB-ключі можуть застосовуватись для служб цифрового підпису з двома ключами – відкритим і закритим. Ці носії можуть використовуватися для безпечного зберігання закритих ключів користувача, а також для безпечного виконання криптографічних перетворень. Хоча дані пристрої не забезпечують абсолютну безпеку, але надійність їхнього захисту набагато перевершує можливості для звичайного настільного комп'ютера.

Високою надійністю і захищеністю відрізняється ідентифікація/автентифікація за допомогою біометричних даних.

Біометрія – сукупність автоматизованих методів ідентифікації й/або автентифікації людей на основі їх фізіологічних і поведінкових характеристик.

Біометричні характеристики можна розділити на дві групи:

1. Фізіологічні біометричні характеристики (фізичні або статичні) – характеристики, засновані на даних, отриманих шляхом вимірювання анатомічних характеристик людини (відбитки пальців, форма обличчя, кисті, структура сітківки й роговиці ока й ін.).

2. Поведінкові біометричні характеристики (також називані динамічними біометричними характеристиками) – біометричні характеристики, що ґрунтуються на даних, отриманих шляхом вимірювання дій людини. Характерною рисою для поведінкових характеристик є їхня довжина в часі (типові приклади – голос, динаміка підпису (ручного), стиль роботи із клавіатурою або мишею).

У загальному вигляді робота з біометричними даними організована в такий спосіб. Спочатку створюється й підтримується база даних характеристик потенційних користувачів. Для цього користувач за допомогою пристрою, що реєструє (наприклад, сканера або камери) надає системі зразок – впізнане, неопрацьоване зображення або запис фізіологічної або поведінкової характеристики. Біометричні характеристики користувача знімаються, обробляються, і результат обробки (біометричний шаблон, або ЕІК – еталонний ідентифікатор користувача) заноситься в базу даних. ЕІК являє собою числову послідовність, при цьому сам зразок неможливо відновити з еталона. Надалі для ідентифікації (і одночасно автентифікації) користувача процес зняття й обробки повторюється, після чого провадиться пошук у базі даних шаблонів. У випадку успішного пошуку

особистість користувача і її автентичність вважаються встановленими. Для автентифікації досить зробити порівняння з одним біометричним шаблоном, обраним на основі попередньо уведених даних.

Оскільки ці два значення (отримане при спробі доступу й ЕІК) повністю ніколи не збігаються (адже біометричні характеристики живої істоти постійно варіюються в певних межах), то для прийняття позитивного рішення про доступ ступінь збігу повинна перевищувати певну граничну величину, що налаштовується. При цьому ефективність біометричних систем характеризується коефіцієнтом помилкових відмов і коефіцієнтом помилкових підтверджень.

Активність розробок в галузі біометрії є дуже значною. Організовано відповідний консорціум (http://www.biometrics.org/), ведуться роботи зі стандартизації різних аспектів технології (формату обміну даними, прикладного програмного інтерфейсу й т.ін.). Застосуванню біометрії сприяє поширення мобільних пристроїв. Так, наприклад, володарі смартфону Samsung Galaxy S5 на території США можуть купувати товари і послуги в Інтернеті на всіх сайтах, що приймають платежі через систему PayPal, з підтвердженням по відбитку пальця. Для цього використовується дактилоскопічний сканер, розміщений на кнопці Home.

Однак, до біометрії варто ставитися досить обережно. Необхідно враховувати, що вона наражається майже на ті ж загрози, що й інші методи автентифікації. Варто враховувати різницю між застосуванням біометрії на контрольованій території, під пильним оком охорони, і в «польових» умовах, коли, наприклад, до пристрою сканування можуть піднести муляж. Біометричні методи не більш надійні, ніж база даних шаблонів, яка може бути ураженою у наслідок атак. До цього слід додати, що біометричні дані людини змінюються з часом, так що база шаблонів має потребу у постійному супроводі, що створює певні проблеми як для користувачів, так і для адміністраторів.

Розвиток технологій дозволяє робити спроби забезпечення ІдА нетрадиційними оригінальними методами. Так компанія Motorola запропонувала використовувати електронні чіпи, які поміщатимуть на або в тіло людини. Одна з реалізацій виконується у вигляді татуювання, що містить кріплення і гнучку мікросхему, яка включає датчик і антену. Інше виконування представлено пілюлями, в яких розміщений електронний чіп, який починає свою роботу внаслідок дії на нього шлункової кислоти після проковтування пілюлі людиною.

З появою інтелектуальних мобільних пристроїв (таких, наприклад, як смартфони) з'явилася можливість використовувати для ІдА двовимірні штрих-коди, які скануються девайсом.

Взагалі штрих-кодова ідентифікація розпочалася з використання виробниками товарів для автоматизації їх руху, зокрема в торгівельних мережах. Потім штрих-кодування знайшло застосування для обліку документів і використання в системах електронного документообігу. Нанесення штрих-коду на паперовий документ значно полегшує процедури зберігання копій документів та їх подальшого пошуку у сховищах.

Лінійний штрих-код, що традиційно використовується, містить невеликий обсяг даних (звичайно не більше 50 байт). Сучасний 2D-код вже підтримує кодування до 2 710 знаків, що розширює сфери його застосування.

Основні недоліки штрих-кодової ідентифікації зводяться до того, що дані ідентифікаційної мітки не можуть доповнюватися – штриховий код записується тільки один раз під час його друку. Дані на мітці представлені у відкритому виді й не захищають від підробок, до того ж штрих-кодові мітки недовговічні.

Штрих-кодова ідентифікація починає витіснятися технологією *радіочастотної ідентифікації – RFID* (Radio frequency identification Device), що інтенсивно впроваджується в багатьох галузях. Радіочастотне розпізнавання здійснюється за допомогою закріплених за об'єктом спеціальних міток, що несуть ідентифікаційну та іншу інформацію. RFID дозволяє одержувати інформацію про предмет ідентифікації без прямого контакту. Дистанції, на яких може відбуватися зчитування й запис інформації, можуть варіюватися від декількох міліметрів до декількох метрів залежно від використовуваних радіочастот.

RFID-системи застосовуються в різноманітних випадках, у тому числі й для електронного контролю за доступом і переміщеннями персоналу на території підприємства, тобто для забезпечення безпеки.

3.2.4. Керування доступом

Після успішного проходження суб'єктом (користувачі й процеси) процедур ІдА починають діяти засоби керування доступом, що дозволяють специфікувати і контролювати дії, які суб'єкти можуть виконувати над об'єктами (інформацією й іншими ресурсами системи). Мова йде про логічне керування доступом, яке, на відміну від фізичного, реалізується програмними засобами.

Логічне керування доступом – це основний механізм багатокористувацьких систем, покликаний забезпечити конфіденційність і цілісність об'єктів і, певною мірою, їхню доступність (шляхом заборони обслуговування неавторизованих користувачів).

Формальна постановка задачі керування доступом в традиційному трактуванні зводиться до задачі для кожної пари «суб'єкт-об'єкт» з сукупності суб'єктів і об'єктів визначити множину припустимих операцій (можливо, залежну від деяких додаткових умов) і контролювати виконання встановленого порядку.

Питання логічного керування доступом є одним з найскладніших в галузі кібербезпеки. Справа в тому, що саме поняття об'єкта (а тим більше видів доступу) розрізняється для кожного виду сервісу. Для операційної системи до об'єктів відносяться файли, пристрої і процеси, хоча сучасні ОС можуть підтримувати й інші об'єкти. Стосовно до файлів і пристроїв зазвичай розглядаються права на читання, запис, виконання (для програмних файлів), іноді на видалення й додавання. Окремим правом може бути можливість передачі повноважень доступу іншим суб'єктам (так зване право володіння). Процеси можна створювати і знищувати. Для систем керування реляційними базами даних об'єкт – це база даних, таблиця, подання, збережена процедура. До таблиць застосовні операції пошуку, додавання, модифікації й видалення даних, в інших об'єктів інші види доступу. Нарешті, труднощі виникають й при експорті/імпорті даних, коли інформація про права доступу, як правило, губиться (оскільки у новому сервісі вона не має сенсу).

При ухваленні рішення про надання доступу зазвичай аналізується наступна інформація:

- ідентифікатор суб'єкта (ідентифікатор користувача, мережна адреса комп'ютера й т.ін.). Подібні ідентифікатори є основою довільного (або дискреційного) керування доступом;
- атрибути суб'єкта (мітка безпеки, група користувача й т.п.). Мітки безпеки – основа примусового (мандатного) керування доступом.

Права доступу у довільному керуванні доступом фіксуються у *матриці доступу*. Але через її розрідженість (більшість комірок є порожніми), зазвичай її зберігають по стовпцях, тобто для кожного об'єкта підтримується список «допущених» суб'єктів разом з їхніми правами. Подібні списки доступу є винятково гнучким засобом, за допомогою якого легко подолати проблему неоднорідної «зернистості» прав.

Але тут має місце недолік, який полягає у тому, що права доступу існують окремо від даних. Ніщо не заважає користувачу, що має доступ до конфіденційної інформації, записати її у файл, який доступний усім. Подібне «розділення» прав і даних істотно ускладнює проведення кількома системами погодженої політики безпеки та, головне, робить практично неможливим ефективний контроль погодженості.

Щодо подання матриці доступу необхідно ще зазначити, що для цього можна використати також функціональний спосіб, коли матрицю не зберігають у явному виді, а щораз обчислюють уміст відповідних комірок.

Зручною надбудовою над засобами логічного керування доступом є *обмежуючий інтерфейс*, коли користувача позбавляють самої можливості спробувати зробити несанкціоновані дії, включивши в число видимих йому об'єктів тільки ті, до яких він має доступ. Подібний підхід зазвичай реалізують у рамках системи меню (користувачу показують лише припустимі варіанти вибору).

При великій кількості користувачів традиційні підсистеми керування доступом стають украй складними для адміністрування. Кількість зв'язків у них зростає пропорційно добутку кількості користувачів на кількість об'єктів. Можливим рішенням в об'єктно-орієнтованому стилі, здатним цю складність понизити, є, як вказувалося, рольове керування доступом.

Рольове керування доступом, згідно зі стандартом рольового керування доступом, розробленим Національним інститутом стандартів і технологій США, оперує наступними основними сутностями:

- користувач (людина, процес і т.п.);
- сеанс роботи користувача;
- роль (звичайно визначається відповідно до організаційної структури персоналу системи);
- об'єкт (сутність, доступ до якої розмежовується; наприклад, файл ОС або таблиця СКБД);
- операція (залежить від об'єкта; для файлів ОС – читання, запис, виконання й т.п.; для таблиць СКБД – вставка, вилучення й т.ін.);
- право доступу (дозвіл виконувати певні операції над певними об'єктами).

Ролям приписуються користувачі й права доступу; можна вважати, що вони (ролі) іменують відношення «багато до багатьох» між користувачами й правами. Ролі можуть бути приписані багатьом користувачам; один користувач може бути приписаний декільком ролям. Під час сеансу роботи користувача активізується підмножина ролей, яким він приписаний, у результаті чого він стає власником об'єднання прав, приписаних активним ролям. Одночасно користувач може відкрити кілька сеансів.

Між ролями може бути визначене відношення часткового порядку, називане *спадкуванням.* Якщо роль r2 є спадкоємицею r1, то усі права r1 приписуються r2, а всі користувачі r2 приписуються r1.

Відношення спадкування є ієрархічним, причому права доступу й користувачі поширюються по рівнях ієрархії назустріч один одному. Можна уявити собі формування ієрархії ролей, починаючи з мінімуму прав (і мак-

симуму користувачів), приписуваних ролі «співробітник», з поступовим уточненням складу користувачів і додаванням прав (ролі «керівник», «бухгалтер» і т.ін.).

Для реалізації ролевого доступу вводиться поняття розділення обов'язків, причому у двох видах: статичному й динамічному. Статичне розділення обов'язків накладає обмеження на приписування користувачів ролям. У найпростішому випадку членство в деякій ролі забороняє приписування користувача певній множині інших ролей. Динамічне розділення обов'язків відрізняється від статичного тільки тем, що розглядаються ролі, одночасно активні для даного користувача (навіть у різних сеансах).

Значних труднощів викликають вирішення питань керування доступом у розподіленому мережному середовищі. Розглянемо це на прикладі використання аплетів, написаних на мові Java.

Аплети – невеликі додатки, написані на різних мовах програмування, які автоматично завантажуються з Інтернету й виконуються сучасними браузерами.

Програми на Java можуть бути трансльовані в байт-код, виконуваний на віртуальній джава-машині (JVM) – програмі, що обробляє байтовий код і передає інструкції обладнанню, як інтерпретатор.

Модель безпеки Java розпочалася з концепції *«пісочниці» (sandbox)* – замкнутого середовища, у якому виконуються потенційно ненадійні програми (аплети, що надійшли з мережі). Програми, що розташовуються на локальному комп'ютері, вважалися абсолютно надійними, і їм було доступно все, що доступно віртуальній Java-машині. У число обмежень, що накладаються «пісочницею», входить заборона на доступ до локальної файлової системи, на мережну взаємодію з усіма хостами, крім джерела аплету, і т.ін. Незалежно від рівня безпеки, що досягається при цьому, (а проблеми виникали й з розділенням свій/чужий, і з визначенням джерела аплету), накладені обмеження варто визнати занадто обтяжними: можливості для змістовних дій в аплетів майже не залишається.

Щоб упоратися із цією проблемою, увели розділення джерел (точніше, розповсюджувачів) аплетів на надійні і ненадійні (джерело визначалося по електронному підпису). Надійні аплети прирівнювалися в правах до «рідного» коду. Зроблене послаблення вирішило проблеми тих, кому прав не вистачало, але захист залишився неешелонованим й, отже, неповним.

Тому від моделі «пісочниці» відмовилися. Оформилися три основних поняття – джерело програми; право й множина прав; політика безпеки.

Джерело програми визначається парою (URL, розповсюджувачі програми). Останні задаються набором цифрових сертифікатів. Java-програми виступають не від імені користувача, що їх запустив, а від імені джерела програми. Це досить глибоке й прогресивне трактування. По-перше, немає поняття власника ресурсів, що міг би змінювати права; останні задаються винятково політикою безпеки (формально можна вважати, що власником усього є той, хто формує політику). По-друге, механізми безпеки наділені об'єктною обгорткою.

Досить важливим поняттям у цій моделі безпеки є *контекст виконання,* який реалізує принцип мінімізації привілеїв. Коли віртуальна Java-машина перевіряє права доступу об'єкта до системного ресурсу, вона розглядає не тільки поточний об'єкт, але й попередні елементи стека викликів. Доступ надається тільки тоді, коли потрібним правом володіють всі об'єкти в стеці.

Контрольні запитання та завдання

1. Роз'ясніть роль ідентифікації та автентифікації як засіб захисту від НСД.

2. Які сутності може пред'явити суб'єкт, що намагається отри-мати доступ до СППР, для підтвердження своєї автентичності?

3. Які причини утруднюють забезпечення надійної ІдА?

4. Приведіть основну класифікацію технологій ідентифікації й автентифікації, що можуть знайти застосування в СППР.

5. Поясніть технологію парольної автентифікації, її переваги та недоліки.

6. У чому полягають переваги застосування одноразових паро-лів?

7. Назвіть апаратні реалізації одноразових паролів.

8. Охарактеризуйте технологію ідентифікації/автентифікації за допомогою біометричних даних.

9. Для чого в СППР може застосовуватись штрих-кодова іден-тифікація, а для чого – радіочастотна?

10. Поясніть призначення засобів керування доступом.

11. Яка інформація аналізується при прийнятті рішення про надання доступу, як вона зазвичай подається?

12. Наведіть основні положення рольового керування доступом.

13. Які труднощі виникають при вирішенні питань керування доступом у розподіленому мережному середовищі?

3.3. ПРОТОКОЛЮВАННЯ Й АУДИТ

Моніторинг систем кібербезпеки. Протоколювання й аудит. Активний аудит.

3.3.1. Моніторинг систем кібербезпеки

Для будь-якої СППР, навіть незначною за кількістю виконуваних функцій, з точки зору забезпечення безпеки необхідні автоматичні й безперервно діючі засоби контролю обладнання, стану мережі, своєчасного оповіщення про можливі проблеми. Адже навіть випадкові збої апаратного або програмного забезпечення можуть привести до досить неприємних наслідків. Що вже казати про випадки, коли критично важливі сервіси або додатки повністю припиняють функціонування.

Ненавмисні відмови обладнання та ПЗ у більшості випадків є разовими і є ситуаціями, що виправляються легко. Значно більшої шкоди можуть принести свідомі шкідливі дії з середини або ззовні мережі. Оскільки повністю виключити подібні сценарії неможливо, рішення полягає у тому, щоб виявляти проблеми на найбільш ранніх стадіях, і отримувати про них найбільш докладну інформацію. Для цього, як правило, застосовується різне ***ПЗ моніторингу і контролю*** системи в цілому та мережі зокрема, що здатне як вчасно сповіщати технічних фахівців про виявлену проблему, так і накопичувати статистичні дані про стабільність й інші параметри роботи серверів, сервісів і служб, доступні для подальшого аналізу.

Типова послідовність процедур забезпечення захисту в СППР з застосуванням засобів моніторингу показана на рис. 3.3.

Вибір способів і об'єктів моніторингу системи та мережі залежить від множини факторів – конфігурації системи, сервісів, що діють у ній і служб, конфігурації серверів і встановленого на них ПЗ, можливостей ПЗ, що використовується для моніторингу й т.ін. На самому загальному рівні можна говорити про такі елементи як:

- перевірка фізичної доступності обладнання;
- перевірка стану (працездатності) служб і сервісів;
- детальна перевірка не критичних, але важливих параметрів функціонування системи – продуктивності, завантаження й т.ін.;

- перевірка параметрів, специфічних для сервісів і служб даного конкретного оточення (наявність деяких значень у таблицях БД, уміст лог-файлів, тощо).

Загальні напрями моніторингу наведені на рис. 3.4.

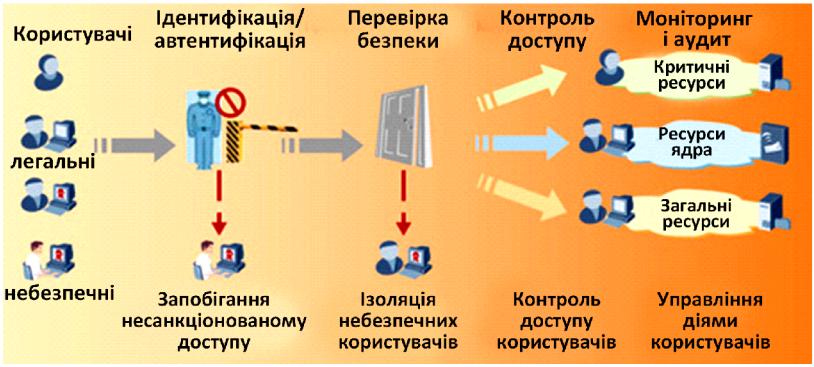


Рис. 3.3. Типова послідовність процедур забезпечення захисту в СППР

Початкові дії з перевірки можуть полягати у тестуванні фізичної доступності обладнання, яка може бути порушеною в результаті відключення самого обладнання або відмови каналів телекомунікацій. Наступний етап – це перевірка працездатності критичних служб. У більшості випадків бажано перевіряти не лише факт відповіді служби або сервісу, але й затримки відповіді. Втім, це відноситься вже до наступній по важливості задачі – перевірці навантаження. Крім часу відгуку пристроїв і служб для різних типів серверів існують інші принципово важливі перевірки – пам'ять і завантаженість процесора веб-сервера, сервера БД, місце на диску файл-сервера. Нарешті, чимало оточень вимагають специфічних перевірок – запитів до БД, що контролюють роботу якогось додатка; перевірка файлів звітів або значень налаштувань; відстеження наявності деякого файлу (наприклад, створюваного при «падінні» системи).

Сутність моніторингу безпеки мережі полягає у виявленні аномальних подій у її функціонуванні. Передбачається, що базові методи забезпечення й контролю безпеки (автентифікація, фільтрація запитів за адресою клієнта, захист від перевантажень і т.ін.) убудовані в усе серверне ПЗ. Однак, по-перше, не завжди можна довіряти цьому припущенню; по-друге, не завжди такого захисту достатньо. Для повноцінної впевненості у безпеці мережі в більшості випадків необхідно використовувати додаткові, зовнішні засоби.

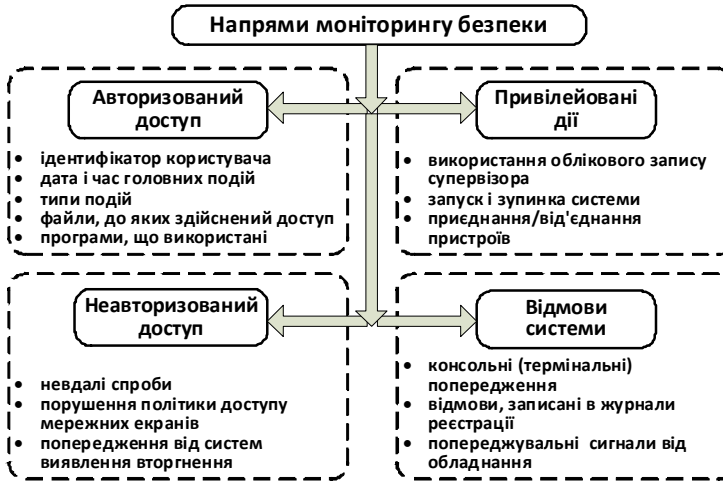


Рис. 3.4. Загальні напрями моніторингу безпеки СППР

При цьому перевіряють, як правило, низку параметрів. Аномально високі рівні завантаження процесора, раптове скорочення вільного місця на дисках, різке збільшення мережного трафіку найчастіше є ознаками мережної атаки. Нагромадження повідомлень про помилки в лог-файлах серверів або журналі подій серверної ОС допомагає виявити повторювані або систематичні відмови. Нарешті, небажані зміни прав доступу до деякого ресурсу або вмісту файлу можуть свідчити про проникнення зловмисника.

У багатьох випадках аномалії, помічені при моніторингу, вимагають негайної реакції технічних фахівців, відповідно, засіб моніторингу повинен мати широкі можливості для пересилання оповіщень (пересилання повідомлень у локальній мережі, електронною поштою у розподіленій мережі).

Необхідно зазначити, що розробка програмної системи моніторингу великої СППР та мережі й контролю її безпеки, вибір необхідної кількості й типів перевірок є серйозною інженерною задачею, що вимагає ретельного підходу. При цьому, конфігуруючи систему моніторингу слід враховувати дві протилежні вимоги: необхідно здійснювати достатню кількість перевірок для забезпечення високого ступеня надійності моніторингу, водночас не занадто захопитися цією кількістю, щоб уникнути перевантажень обладнання та фахівців, у чиї обов'язки буде входити аналіз результатів моніторингу.

Прикладом готового продукту забезпечення моніторингу стану мережі й контролю її безпеки є програма Alchemy Eye. Цей засіб дозволяє

створювати будь-яку кількість об'єктів моніторингу. В Alchemy Eye доступні перевірки фізичної доступності обладнання, працездатності служб і сервісів, запущених у мережі, навантаження мережі й окремих служб, специфічних параметрів (наприклад, SQL-запитів) та ін.

3.3.2. Протоколювання й аудит

Інформація, накопичена під час моніторингу подій в системі, підлягає реєстрації і подальшого аналізу. Для цього застосовуються засоби протоколювання й аудиту.

Протоколювання – збір і нагромадження інформації про події, що відбуваються в інформаційній системі.

Аудит – аналіз накопиченої інформації, проведений оперативно, у реальному часі або періодично (наприклад, раз у день).

Активний аудит – оперативний аудит з автоматичним реагуванням на виявлені позаштатні ситуації.

Аудит інформаційної безпеки – аналіз системи інформаційної безпеки підприємства на відповідності вимогам міжнародних стандартів до інформаційних систем в галузі забезпечення захисту.

Реалізація протоколювання й аудита вирішує наступні завдання:

- забезпечення підзвітності користувачів і адміністраторів;
- забезпечення можливості реконструкції послідовності подій;
- виявлення спроб порушень інформаційної безпеки;
- надання інформації для виявлення й аналізу проблем.

Протоколювання вимагає для своєї реалізації вирішення питань щодо того, які події реєструвати та з яким ступенем деталізації це робити. Розумний підхід до вказаних питань пропонується в «Оранжевій книзі», де виділені наступні події:

- вхід у систему (успішний чи ні);
- вихід із системи;
- звернення до віддаленої системи;
- операції з файлами (відкрити, закрити, перейменувати, видалити);
- зміна привілеїв або інших атрибутів безпеки (режиму доступу, рівня благонадійності користувача й т.ін.).

При протоколюванні події рекомендується записувати, принаймні, наступну інформацію:

- дата й час події;

- унікальний ідентифікатор користувача – ініціатора дії;
- тип події;
- результат дії (успіх або невдача);
- джерело запиту (наприклад, ім'я термінала);
- імена зачеплених об'єктів (наприклад, файлів, що відкривають або вилучають);
- опис змін, внесених у бази даних захисту (наприклад, нова мітка безпеки об'єкта).

Ще одним важливим поняттям, що фігурує в «Оранжевій книзі», є *вибіркове протоколювання* – як відносно користувачів (уважно стежити тільки за підозрілими), так і відносно подій. Забезпечення підзвітності, яке реалізується засобами протоколювання й аудита, є важливим в першу чергу як стримуючий засіб. Якщо користувачі й адміністратори знають, що всі їхні дії фіксуються, вони, можливо, утримаються від незаконних операцій.

В розподіленій різнорідній системі здійснити організацію погодженого протоколювання й аудита дуже непросто. По-перше, деякі компоненти, важливі для безпеки (наприклад, маршрутизатори), можуть не мати власних ресурсів протоколювання; у такому випадку їх потрібно екранувати іншими сервісами, які візьмуть протоколювання на себе. По-друге, необхідно погоджувати між собою події в різних сервісах і в різних вузлах мережі.

Роботи щодо аудита безпеки системи зазвичай виконуються в декілька етапів, передбачених програмою безпеки.

До таких етапів відносяться постановка задачі й визначення об'єкта аудита, збір, підготовка й аналіз даних для проведення робіт, підготовка аналітичного звіту з виконаної роботі, нарешті, доведення результатів до відповідного персоналу підприємства. Деталізація етапів аудита проводиться робочою групою експертів на етапі підготовки технічного завдання на виконання робіт.

3.3.3. Активний аудит

Якщо традиційно аудит проводиться періодично або у разі необхідності, то завдання активного аудита – оперативно, як правило, у режимі реального часу виявляти підозрілу активність і надавати засоби для автоматичного реагування на неї. Під *підозрілою активністю* розуміється поведінка користувача або компонента системи, що може бути злочинною (відповідно до заздалегідь визначеної політики безпеки) або нетиповою (відповідно до прийнятих критеріїв).

Для опису й виявлення атак можна застосовувати універсальні методи, такі як сигнатури і їхнє виявлення у вхідному потоці подій за допомогою апарата експертних систем.

Сигнатура атаки – сукупність умов, при виконанні яких атака вважається такою, що має місце, і що викликає заздалегідь певну реакцію.

Найпростіший приклад сигнатури – «зафіксовані три послідовні невдалі спроби входу в систему з одного термінала», приклад асоційованої реакції – блокування термінала до прояснення ситуації.

Нетипова поведінка виявляється статистичними методами. У найпростішому випадку застосовують систему порогів, перевищення яких є підозрілим. Втім, такий «граничний» метод можна трактувати і як вироджений випадок сигнатури атаки, і як тривіальний спосіб виразу політики безпеки.

Стосовно до засобів активного аудита розрізняють помилки першого й другого роду, а саме пропуск атак і фіктивні тривоги, відповідно. Небажаність помилок першого роду є очевидною; помилки другого роду не менш неприємні, оскільки відволікають адміністратора безпеки від дійсно важливих справ, побічно сприяючи пропуску атак.

Переваги сигнатурного методу – висока продуктивність, мале число помилок другого роду, обґрунтованість рішень.

Основний недолік – невміння виявляти невідомі атаки та варіації відомих атак.

Основні переваги статистичного підходу – універсальність і обґрунтованість рішень, потенційна здатність виявляти невідомі атаки, тобто мінімізація числа помилок першого роду. Негатив полягає у відносно високій частці помилок другого роду, поганій роботі у випадку, коли неправомірна поведінка є типовою, коли типова поведінка плавно змінюється від легальної до неправомірної, а також у випадках, коли типової поведінка немає взагалі – є й такі користувачі.

Засоби активного аудита можуть розташовуватися на всіх лініях оборони СППР. На межі контрольованої зони вони можуть виявляти підозрілу активність у точках підключення до зовнішніх мереж (не тільки спроби нелегального проникнення, але й дії щодо «промацуванню» сервісів безпеки). У корпоративній мережі, у рамках інформаційних сервісів і сервісів безпеки, активний аудит у змозі виявити й припинити підозрілу активність зовнішніх і внутрішніх користувачів, виявити проблеми в роботі сервісів, викликані як порушеннями безпеки, так і апаратно-програмними помилками.

Серед вимог до систем активного аудита на перше місце варто поставити вимогу повноти. Це досить ємне поняття, що включає в себе такі чинник, як повнота відстеження інформаційних потоків до сервісів, по-

внота спектра атак і зловживань повноваженнями, що виявляються, а також достатня продуктивність.

Крім повноти системи активного аудита повинні задовольняти таким вимогам, як мінімум фіктивних тривог, уміння пояснювати причину тривоги, інтеграція із системою керування й інших сервісів безпеки, а також наявність технічної можливості віддаленого моніторингу системи.

У складі засобів активного аудита можна виділити такі функціональні компоненти, як генерації реєстраційної інформації її зберігання та перегляду, аналізу інформації, прийняття рішень і реагування, інтерфейсу з адміністратором безпеки. Основні елементи локальної архітектури систем активного аудита наведені на рис. 3.5.

Засоби активного аудита будуються в архітектурі менеджер/агент.

Основними агентськими компонентами є *сенсори*, що розміщуються на стику між засобами активного аудита й контрольованих об'єктів. Аналіз, прийняття рішень – функції менеджерів. Зрозуміло, що між менеджерами й агентами повинні бути сформовані довірені (надійно захищені) канали.

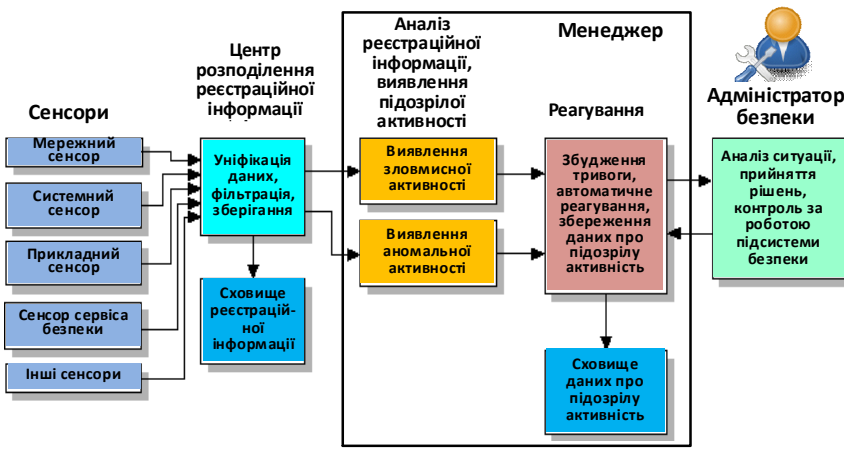


Рис. 3.5. Основні елементи локальної архітектури систем активного аудита

Сенсорі реалізуються у вигляді виділених комп'ютерів, мережні карти яких установлені в режим прослуховування – це зазвичай мережні сервери, або як програми, що читають реєстраційні журнали операційної системи. Останні – це локальні, або хостові сенсори.

Треба звернути увагу на архітектурну спільність засобів активного аудита й моніторингу, що є наслідком єдності виконуваних функцій. Істот-

но полегшити гуртову роботу цих засобів сприяє застосування продуманих інтерфейсних компонент. Вони корисні не лише із зовнішньої точки зору, а й безпосередньо для засобів активного аудита, чим забезпечують розширюваність, підключення компонентів різних виробників і т.ін.

У випадку застосування активного аудиту для СППР з розгалуженими мережами архітектура засобів аудиту набуває ієрархічного вигляду, де добування та аналіз реєстраційної інформації здійснюється окремо по шарам мереж з поступовою консолідацією інформації на вищих щаблях ієрархії. Тим самим формується архітектура комплексної системи аудиту.

Контрольні запитання та завдання

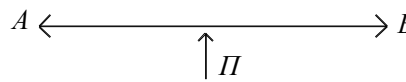
1. Для чого в СППР доцільно застосовувати засоби моніторингу і контролю системи в цілому та мережі (за наявності) зокрема?
2. Поясніть типову послідовність процедур забезпечення захисту в СППР з застосуванням засобів моніторингу.
3. Назвіть можливі основні напрями моніторингу безпеки СППР.
4. Які основні завдання вирішує реалізація протоколювання й аудиту?
5. Яку інформацію, що циркулює в СППР, рекомендується записувати при протоколюванні події?
6. У чому полягає специфіка активного аудиту?
7. Охарактеризуйте архітектурні рішення побудови комплексу засобів активного аудита.

3.4. КРИПТОЛОГІЯ ТА ШИФРУВАННЯ

Поняття криптології. Історична довідка. Шифрування. Алгоритми шифрування. Контроль цілісності

3.4.1. Поняття криптології

Перші спроби захисту інформації були пов'язані з практичної потреби передавати важливі відомості найнадійнішим чином. Ситуацію, в якій виникає задача таємної передачі, ілюструється наступною схемою



Тут *А* і *В* – віддалені законні користувачі інформації, які хочуть обмінюватися інформацією з використанням деякого загальнодоступного каналу зв'язку, але вони прагнуть захистити інформацію.:

П – незаконний користувач (порушник, супротивник), що може перехоплювати передані по каналу зв'язку повідомлення й намагатися витягти з них інформацію, яка його цікавить. Цю формальну схему можна вважати моделлю типової ситуації, у якій для захисту інформації застосовується шифрування.

Ніхто не може сказати точно, коли ж був придуманий найперший шифр на світі. Мабуть, відразу після появи писемності. Більше того, спочатку писемність сама по собі була своєрідною криптографічною системою, оскільки в древніх суспільствах нею володіли лише вибрані.

Швидше за все, шифрування пов'язане з появою державного і військового листування. Сьогодні вже будь-яка людина може зашифрувати дані, які вона завантажує в Мережу, пересилає електронною поштою або вводить в онлайн-форми при проведенні банківських операцій. Але при цьому принципи, на яких базується сучасне шифрування, залишилися старими, як світ. Різниця тільки в тому, що в давні часи кодувалися літери, а сьогодні – блоки бітів.

Таким чином, упродовж тисячоліть з потреби передавати захищену інформацію розвинулася фундаментальна наука – криптогогія.

	Криптологія – наука, що займається методами *шифрування і дешифрування*. Відповідно, криптологія складається із двох частин – *криптографія і криптоаналіз*. **Криптографія** (від грецького *kryptos* – прихований і *graphein* – писати) – наука про математичні методи забезпечення конфіденційності (неможливості прочитання інформації стороннім) і автентичності (цілісності і справжності авторства) інформації. **Криптоаналіз** (від грец. κρυπτός – схований і аналіз) – наука про методи одержання вихідного значення зашифрованої інформації, не маючи доступу до секретної інформації (ключа), необхідної для цього.

Сучасна модель захисту інформації, що передається, з застосуванням шифрування, наведено на рис. 3.6. Відправник генерує відкритий текст вихідного повідомлення *М*, яке має бути передане законному одержувачеві по незахищеному каналу. За каналом стежить перехоплювач з метою перехопити і розкрити повідомлення, що передається. Для того, щоб перехоплювач не зміг дізнатися вмісту повідомлення *М*, відправник шифрує

його за допомогою оборотного перетворення E_K і отримує *шифротекст* (або *криптограму*) $C = E_K(M)$, який відправляє одержувачеві. Законний одержувач, прийнявши шифротекст C, розшифровує його за допомогою зворотного перетворення $D = EK^{-1}$ і отримує вихідне повідомлення у вигляді відкритого тексту M. Перетворення EK вибирається з сімейства криптографічних перетворень, званих *криптоалгоритмами*. Параметр, за допомогою якого вибирається окреме використовуване перетворення, називається *криптографічним ключем К*.

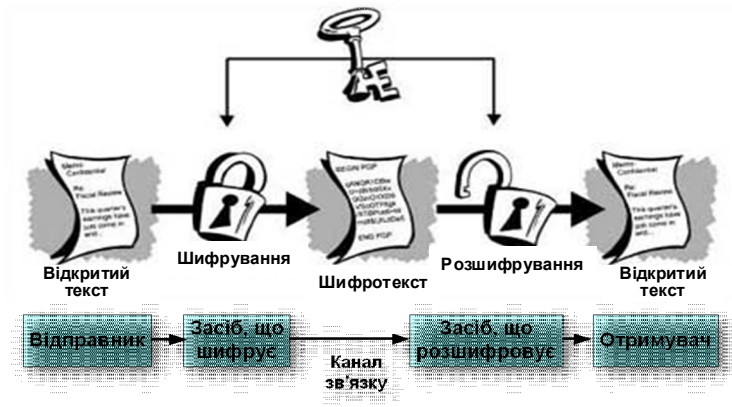


Рис. 3.6. Сучасна модель захисту інформації, що передається, з застосуванням шифрування

Отже, для шифрування тексту вибір конкретного перетворення визначає ключ. У сучасних шифрах алгоритм шифрування є відомим, а стійкість шифру цілком визначається таємністю ключа. Цей принцип уперше сформував відомий вчений голландець А. Керкхофф.

Виходячи з цього принципу, методи порушення конфіденційності і цілісності інформації без знання ключа, в основному математичні, сформувалися в розділ криптології – криптоаналіз. Простіше кажучи, криптоаналіз – це *взламування коду*. Цей термін був уведений «батьком американської криптографії» Уїльямом Ф. Фрідманом ще у 1920 році. Спроба криптоаналітика викликати відхилення в захищеній системі, отримала назву *криптографічна атака*. Успішну криптографічну атаку називають злом, або розкриття.

Але під терміном «криптоаналіз» також розуміється і більш шляхетна задача – спроба знайти уразливість у криптографічному алгоритмі або протоколі з метою його подальшого вдосконалення, тобто підвищити його *криптографічну стійкість*.

	Зашифрування – процес нормального застосування криптографічного перетворення відкритого тексту на основі алгоритму і ключа, в результаті якого виникає шифрований текст. **Розшифрування** – процес нормального застосування криптографічного перетворення шифрованого тексту у відкритий зі знанням криптографічного ключа. **Дешифрування** – процес добування вихідного тексту без знання криптографічного ключа на основі відомого зашифрованого тексту.

Протягом багатьох століть серед фахівців і вчених не вщухали суперечки про стійкість шифрів і про можливість побудови абсолютно стійкого шифру. Поки ще такого не знайдено, і на практиці застосовуються *неабсолютно стійкі шифри*. Такі шифри, в принципі, можуть бути розкриті. Питання лише у тому, чи вистачить у супротивника (криптоаналітика) сил, засобів і часу для розробки й реалізації відповідних алгоритмів. Вважається, що криптоаналітик з необмеженими ресурсами може розкрити будь-який неабсолютно стійкий шифр.

3.4.2. Шифрування та історія розвитку

Для сучасної криптографії характерне використання відкритих алгоритмів шифрування. Відомо більш десятка перевірених алгоритмів шифрування, які, при використанні ключа достатньої довжини і коректної реалізації алгоритму, забезпечують недоступність шифрованого тексту для криптоаналізу. Загальну класифікацію алгоритмів шифрування наведено на рис. 3.7.

Як же розвивалася криптографія упродовж тисячоліть? Її історія є дуже повчальної для опанування початків шифрування.

Довгий час заняття криптографією було долею диваків-одинаків. Серед них були політичні діячі, дипломати, талановиті вчені, священнослужителі. Криптографія вважалася навіть чорною магією. Цей період розвитку криптографії як мистецтва тривав з незапам'ятних часів до початку XX століття. З математичної точки зору первісну історію криптографії можна назвати наївною, і лише з кінця XV ст. її можна віднести до формальної криптографії.

Перші спроби прихованої передачі повідомлень, що відносяться до 440 року до н. е., пов'язані з тайнописом, при якому повідомлення закодоване таким чином, що не виглядає як повідомлення – на відміну від

криптографії. Таким чином непосвячена людина принципово не може розшифрувати повідомлення – бо не знає про факт його існування. Це поняття пізніше отримало синонім *стеганографія* (від грецької *στεγανος* – прихований + *γραφω* – пишу).

Рис. 3.7. Загальна класифікація алгоритмів шифрування

Один з давніх спосіб тайнопису полягав у наступному: на поголену голову раба записувалося необхідне повідомлення, а коли його волосся відростало, він вирушав до адресата, який знову голив його голову і зчитував доставлене повідомлення. Такі екзотичні методи, звісно, канули в історію, і зараз, з появою комп'ютерів, стеганографія отримала більш витончені алгоритми – від роздрукування на принтері текстів з малопомітними викривленнями обрисів окремих символів тексту до створення цифрових водяних знаків, які, на відміну від звичайних, можна нанести і відшукати тільки за допомогою спеціального програмного забезпечення.

Якщо стеганографія приховує сам факт існування повідомлення, то криптографія приховує зміст повідомлення. За свідченнями дослідників єгипетських пірамід під час розкопок були виявлені склепи з дуже дивними написами. Там одні ієрогліфи замінялися на інші. Приклади шифровок можна знайти й у Біблії – так, цар Вавилона завдяки перестановки алфавіту навпаки (перша літера стала останньої, друга – передостанньої й т.д.) перетворився в царя Сессах. У тій же книзі згадується й нагорода «першому криптоаналітику» – пророка Данила за прочитання загадкового напису вдягли в багряницю й проголосили третім владарем царства.

Зрозуміло, що шифри тих часів були примітивні. Замінялися літери, фрази, поняття, так що повідомлення або легко піддавалися дешифруванню навіть без знання ключа, або не розшифровувалися взагалі.

Найдавнішими з криптографічних алгоритмів є алгоритми шифрування *заміною (підстановкою)* та шифрування *перестановкою*. Перше полягає в тому, що символи тексту, що шифрується, замінюються символами того ж або іншого алфавіту відповідно до заздалегідь обумовленої схеми заміни. У тому випадку, коли використовується лише один алфавіт, система заміни називається однолфавітною (моноалфавітною). Коли застосовуються два або більше алфавітів за якимсь заздалегідь визначеним правилом, система заміни стає багато алфавітною, або поліалфавітною.

Суть другого алгоритму полягає в тому, що символи тексту, що шифрується, переставляються за певним правилом в межах деякого блоку цього тексту. Перетасувати букви слова «секрет» так, щоб отримати, наприклад, «еткрсе», і означає зробити перестановку. При достатній довжині блоку, в межах якого здійснюється перестановка, і складному порядку перестановки, що не повторюється, можна досягти прийнятної для простих практичних застосувань стійкості шифру.

Об'єднує ці алгоритми важлива особливість – використання одного і того ж ключа для шифрування і розшифрування, від чого ці алгоритми отримали назву *симетричних*. Асиметричні алгоритми були винайдені лише у XX ст. Вони передбачають використання вже двох ключів. Про це ми поговоримо пізніше, адже початок історії пов'язаний саме з симетричними алгоритмами.

Перший шифр перестановки (шифр «Сцитала» відомий із часів війни Спарти проти Афін у V столітті до н.е. Для його реалізації використовувалася сцитала – жезл, що має форму циліндра. На нього намотувалася смуга, на яку наносилися літери тексту. Після розмотування смуги текст можна було прочитати лише намотавши його на жезл саме такого ж діаметру (це власне й є ключ шифрування). Але старогрецький учений Аристотель (384-322 до н. е.) спромігся винайти спосіб розкриття шифру «сцитала».

Римський імператор і полководець Цезар (50 років до н. е.) захищав свою кореспонденцію, здвигаючи літери на визначену кількість позицій (шифр заміни, або підстановками). Наприклад, на алфавіті A B C D E F G H I J K L M N O P Q R S T U V W X Y Z з ключем 3 маємо:

A → D	J → M	S → V
B → E	K → N	T → W
C → F	L → O	U → X
D → G	M → P	V → Y
E → H	N → Q	W → Z
F → I	O → R	X → A
G → J	P → S	Y → B
H → K	Q → T	Z → C
I → L	R → U	

Тоді вихідний текст SECRET перетворюється у шифрований текст: VHFUHW. Незважаючи на популярність і фундаментальність шифру Цезаря, він має суттєві недоліки. По-перше, це замало ключів – на одиницю менше, ніж літер в абетці. Але, що важніше – частота появи кожної літери в шифротексті співпадає з частотою появи у відкритому тексті! Як відомо, частота використання літер у текстах на конкретній мові є досить сталою (наприклад. на рис. 3.8. наведено гістограму частот літер в англійському тексті). Саме за допомогою частотного аналізу груп кріптоаналітики знаходять літери ключа.

Підвищити стійкість системи шифрування Цезаря можна з використанням ключового слова. Нехай вибрано слово DIPLOMAT як ключове слово і число к = 5. Ключове слово записується під буквами алфавіту, починаючи з букви, числовий код якої збігається з вибраним числом к (починаючи з нуля). Букви алфавіту підстановки, що залишилися, записуються після ключового слова в алфавітному порядку:

					5																			
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
V	W	X	Y	Z	D	I	P	L	O	M	A	T	B	C	E	F	G	H	J	K	N	Q	R	S	U

Тоді вихідне повідомлення SEND MORE MONEY шифрується як HZBY TCGZ TCBZS.

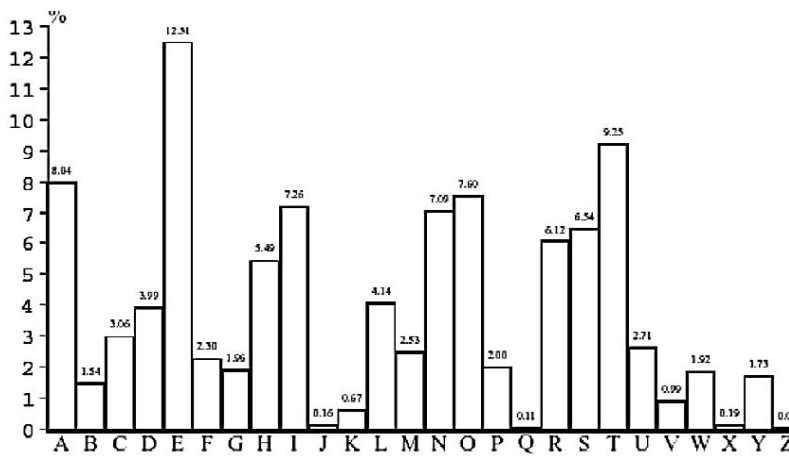


Рис. 3.8. Гістограма частот літер в англійському тексті

Це удосконалення шифру Цезаря зробив француз Віженер у XVII ст., заклавши основу поліалфавітного шифрування, яке дуже важко піддаєть-

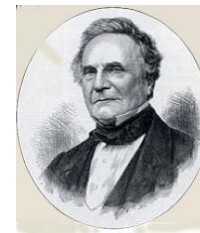
ся злому. Зламування цього коду можливе також на основі частотного аналізу, але потрібно знати частоту комбінацій букв, що йдуть підряд. Одним з перших, хто розгадав достатньо складний шифр Віженера, був відомий математик Чарльз Беббідж, який зробив це аж у 1854 р.

З часів середньовіччя почався формальний етап розвитку систем шифрування, а само шифрування від мистецтва вже перейшло у стан ремесла. «Батьком» європейської криптології та формального етапу вважається Леон Батиста Альберті (1404-1472), італійський архітектор. Саме він у своїй праці «Трактат про шифри» (1466 р.) вперше запропонував шифр поліалфавитної заміни, який робив повідомлення практично не розкривним. У цій роботі був запропонований шифр, заснований на використанні *шифрувального диска*.

З XV ст. надійшли відповідні праці Леонардо да Вінчі, а одну з перших книг по криптографії написав абат Трителій (1462-1516), який жив у Німеччині. У 1566 році відомий математик Д. Кардано опублікував роботу з описом винайденої ним системи шифрування («ґрати Кардано»).

Гай Юлій Цезар, давньоримський державний і політичний діяч, полководець, письменник, автор шифру заміни

Блез де Віженер *(Blaise de Vigenere)*, французький дипломат та криптограф, автор поліалфавітного шифру, який у якості ключа використовує слово

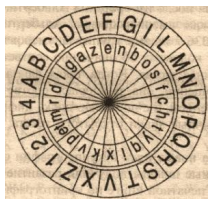


Чарлз Беббідж *(Charles Babbage)*, англійський математик, винахідник першої обчислювальної машини, першим розшифрував шифр Віженера

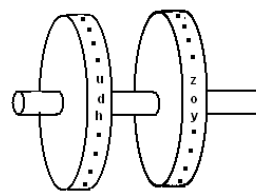
Розвиток криптографії супроводжувався появою та постійним вдосконаленням технічних засобів, що використовувались для реалізації шифрів та для їх розкриття. Томас Джефферсон, третій президент США, 1790 року передбачив винахід ще одного широко відомого шифрувального пристрою – циліндра. Цей пристрій складався з декількох дисків (до 40), що оберталися, закріплені на загальній осі. На кожен диск була нанесена своя (причому перемішана) алфавітна послідовність.

Такі засоби, як і шифрувальні диски, у XX ст. використовувались у складі механічних обчислювальних машин, як німецька «Енігма», що застосовувалась у часи війни 1941-45 років, або «Фіалка» (1965р.) – соціалістична версія «Енігми». До речі, коди «Енігми» були розшифровані спеціалізованою обчислювальною машиною для перебору ключів «Бомба», спроектована відомим англійським математиком Аланом Тьюрингом 1940 р.

Поява більш складних методів та перехід криптографії у стан науки пов'язані з математичними дослідженнями лише у XX столітті. До засадничих робіт слід віднести працю К. Шеннона «Математична теорія зв'язку» (1948 р.) та роботи щодо криптосистем з відкритим ключем Діффі-Хелмана (1976 р.).



Шифрувальний диск, 1467 р.
Запропонований італійцем Леоном Батиста Альберті (1404-1472)



Шифрувальний циліндр, 1790 р.
Запропонований Томасом Джефферсоном, третім президентом США (1743-1826)

«Енігма»,
німецька шифрувальна машина (1941-45 рр.)

У своїй роботі «Теорія зв'язку в секретних системах» Клод Шеннон узагальнив накопичений до нього досвід розробки шифрів. Виявилося, що навіть у дуже складних шифрах як типові компоненти можна виділити такі прості шифри як шифри заміни, шифри перестановки або їх сполучення.

3.4.3. Сучасний стан криптографії

Для сучасної криптографії характерне використання відкритих алгоритмів шифрування, що передбачають використання обчислювальних засобів. Теперішні алгоритми шифрування мають бути складними для зламування, а також проектуватись з урахуванням неможливості зламування у майбутньому. Відомо більш десятка перевірених алгоритмів шифрування, які, при використанні ключа достатньої довжини і коректної реалізації

алгоритму, забезпечують недоступність шифрованого тексту для криптоаналізу. Що стосується безпечної довжини ключа, то, наприклад, на цей час більшість стандартів з RSA визначають довжину у 512 біт, але поступово вже широко вживається довжина у 1024 біта.

У зв'язку із цим необхідно зазначити, що ускладнення алгоритмів і збільшення довжини ключів потребує усе більш потужних комп'ютерів, зокрема для проведення криптоаналізу. Так, наприклад, зараз Агентству національної безпеки США, відомому своїми успіхами у практичному криптоаналізі, належить одна з найпотужніших моделей суперкомп'ютера «Cray-T3D» з кількістю процесорів 1024. Тому майбутнє криптографії і криптоаналізу пов'язують з вдосконаленням технічної комп'ютерної бази, зокрема появою квантових комп'ютерів, здатних розв'язувати криптографічні задачі набагато швидше, ніж звичайні комп'ютери. У квантовій криптографії використовується метод невизначеності Гейзенберга: при перехваті повідомлення воно повністю змінюється і стає нечитабельним.

Але повернемось у сьогодення. На цей час алгоритми шифрування поділяються на симетричні алгоритми, асиметричні алгоритми або їх поєднання.

Особливість симетричних алгоритмів шифрування полягає у тому, що ключ шифрування та розшифрування однаковий (і він зберігається в секреті), тобто за його допомогою (на відміну від асиметричних алгоритмів шифрування) можна як зашифрувати, так і розшифрувати (відновити) повідомлення.

Рис. 3.9 ілюструє використання симетричного шифрування. Хоча ми ведемо мову про захист повідомлень, але, зрозуміло, така ж схема застосовується й, наприклад, для шифрування й розшифрування файлів, що нікуди не переміщуються.

Основним недоліком симетричного шифрування є те, що секретний ключ повинен бути відомим і відправникові, і одержувачеві, тобто необхідно мати секретний ключ у них обох. З одного боку, це створює проблему поширення ключів. З іншого боку, одержувач на підставі наявності зашифрованого й розшифрованого повідомлення не може довести, що він одержав це повідомлення від конкретного відправника, оскільки таке ж повідомлення він міг згенерувати й самостійно.

Оскільки ключі є предметом можливого перехоплення, їх необхідно часто змінювати та передавати по безпечних каналах передачі інформації під час розповсюдження.

Симетричні алгоритми шифрування можна розділити на потокові та блочні. Потокові алгоритми шифрування послідовно обробляють текст повідомлення. Блочні алгоритми працюють з блоками фіксованого розміру. Як правило, довжина блоку дорівнює від 64 біт і більше.

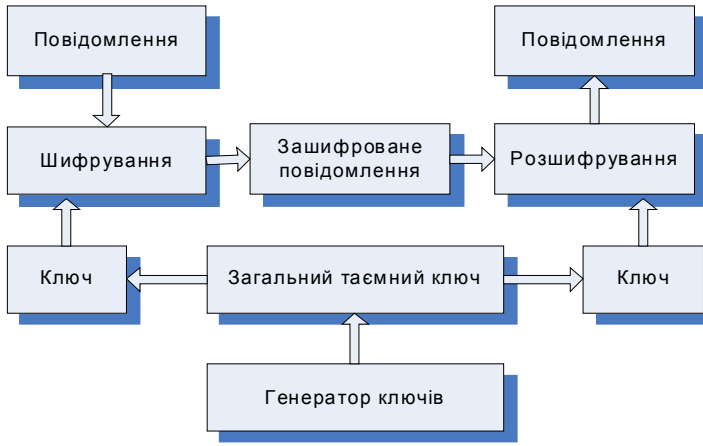


Рис. 3.9. Використання симетричного методу шифрування

У світі напрацьовано чимало стандартних алгоритмів симетричного шифрування. Одним з перших став стандарт DES (Data Encryption Standard), розроблений компанією IBM спільно з Агентством національної безпеки США у 1976р. для використання в органах влади. Він є типовим представником блочного шифрування з довжиною ключа у 56 біт.

У радянські часи на наших теренах був прийнятий стандарт шифрування ГОСТ 28147-89, який побудований з урахуванням DES, але є більш вдосконаленим.

З розвитком комп'ютером стандарти подібні DES сталили не оптимальними. Тепер алгоритм DES рекомендовано використовувати тільки в режимі Triple-DES (3DES). В ньому використовується три підключа довжиною 56x3=168 біт. Шифрування здійснюється в три етапи: шифрування з одним підключем, розшифрування з другим підключем та знов шифрування з третім.

На зміну алгоритмові DES у 2000 р. прийшов стандарт симетричного шифрування AES (Advanced Encryption Standard). Це також блочне шифрування на основі алгоритму Rijndael (Рейндал) зі змінною довжиною ключа 128, 192 і 256 біт та змінною довжиною блоків.

1975 року відбувся революційний винахід у сфері криптографії, який зробив стійку криптографію доступною для масового використання. Проблема керування ключами, що має місце в симетричних алгоритмах, була вирішена Уітфілдом Діффі і Мартіном Хеллман у статті «Нові шляхи криптографії», де була запропонована концепція асиметричних алгоритмів шиф-

рування, які використовують різні ключі для шифрування та дешифрування даних (ця концепція ще має назву криптографії з відкритим ключем).

Криптографія з відкритим ключем – це асиметрична схема, у якій застосовуються пари ключів: відкритий (public key), що зашифровує дані, і відповідний йому закритий (private key), що їх розшифровує.

Ідея полягає у тому, що ви поширюєте свій відкритий ключ по усьому світу (він може публікуватися разом з іншими відкритими відомостями про користувача), у той час як закритий – для розшифрування – тримаєте в таємниці. Будь-яка людина з копією вашого відкритого ключа – хто завгодно, навіть люди, з якими ви ніколи не зустрічалися – може зашифрувати інформацію, яку тільки ви зможете прочитати.

Схему використання асиметричного шифрування наведено на рис. 3.10.

Прикладами криптосистем з відкритим ключем є Diffie-Hellman (названа на честь авторів), Elgamal (названа на честь автора Тахіра Ельгамаля), RSA (названа на честь винахідників Рона Рівеста, Аді Шаміра і Леонарда Аделмана), DSA – Digital Signature Algorithm (винайдений Девідом Кравіцом).

Криптосистема з відкритим ключем повністю визначається трьома алгоритмами: генерації ключів, шифрування та дешифрування. Алгоритм генерації ключів G є загальнодоступним; усякий бажаючий може подати йому на вхід випадковий рядок r належної довжини і отримати пару ключів K_1, K_2. Відкритий ключ K_1 публікується, а секретний ключ K_2 і випадковий рядок r зберігаються в секреті. Алгоритми шифрування E_{K1} й дешифрування D_{K2} такі, що якщо (K_1, K_2) – пара ключів, згенерованих алгоритмом G, то $D_{K2}(E_{K1}(m))$ для будь-якого відкритого тексту m.

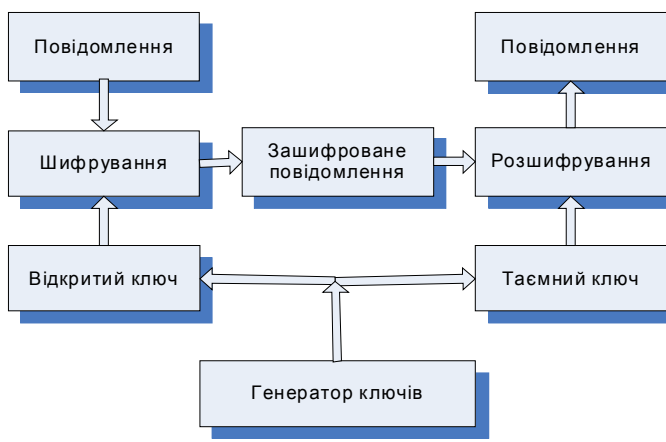


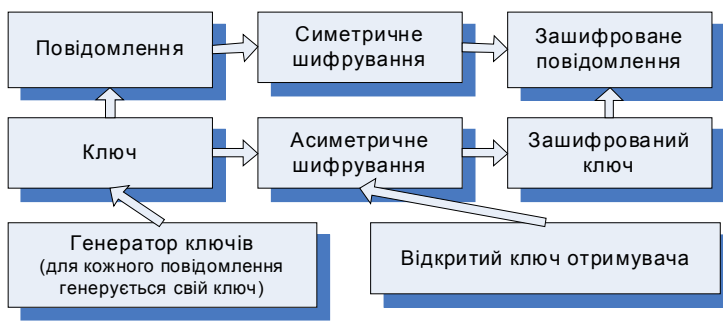
Рис. 3.10. Використання асиметричного методу шифрування

Таким чином, хоча ключова пара є математично зв'язаною, обчислення закритого ключа з відкритого практично є нездійсненним. Кожний, у кого є відкритий ключ, зможе зашифрувати дані, але не зможе їх розшифрувати. Тільки людина, яка володіє відповідним закритим ключем може розшифрувати інформацію.

Родзинкою нової ідеї була пропозиція застосувати для шифрування однобічні функції. Функції такі були відомі математикам ще з часів фараонів. Вони мають наступну властивість: при заданому значенні x відносно просто обчислити значення $y = f(x)$, однак немає простого шляху для обчислення значення x з відомого y, навіть якщо сама функція є відомою. Але якщо відомим є якийсь «секретний шлях», то знаходження x не викликає труднощів.

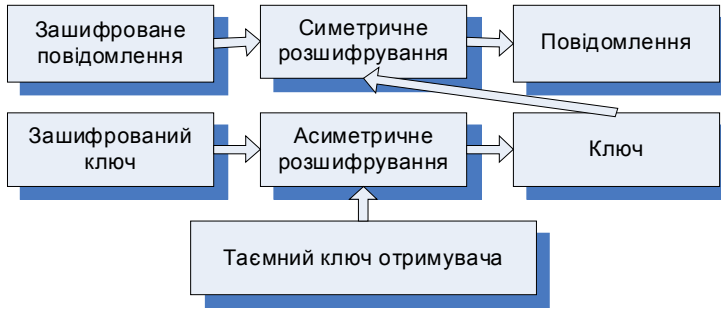
Тобто однобічна функція – це ефективно обчислювальна функція, для задачі інвертування якої не існує ефективних алгоритмів. Під інвертуванням розуміється масова задача знаходження за заданим значенням функції одного (кожного) значення із прообразу (помітимо, що зворотна функція, взагалі кажучи, може й не існувати). Для практичних цілей криптографії було побудовано кілька функцій, які можуть виявитися функціями із секретом. Найбільш відомою й популярною з них є теоретико-числова функція, на якій побудований шифр RSA.

Але й асиметричні методи шифрування не позбавлені недоліків, найістотнішим з яких є їхня низька швидкодія (асиметричні методи на 3 – 4 порядки повільніше симетричних). Тому дані методи доводиться сполучати із симетричними (рис. 3.11).



а)

Рис. 3.11. Використання асиметричного та симетричного методу шифрування (а – ефективне шифрування повідомлення)



б)

Рис. 3.11. Використання асиметричного та симетричного методу шифрування (б – його розшифрування)

Так, для розв'язання задачі ефективного шифрування з передачею секретного ключа, використаного відправником, повідомлення спочатку симетрично зашифровують випадковим ключем, потім цей ключ зашифровують відкритим асиметричним ключем одержувача, після чого повідомлення й ключ відправляються по мережі.

Необхідно також зазначити, що асиметричні методи дозволили розв'язати важливу задачу спільного вироблення секретних ключів, що обслуговують сеанс взаємодії, при початковій їх відсутності (це є суттєвим, якщо сторони не довіряють один одному) Для цього використовується алгоритм Діффи-Хелмана.

3.4.4. Контроль цілісності

Криптографічні методи дозволяють не лише надійно закривати повідомлення, але й контролювати цілісність як окремих порцій даних, так і їхніх наборів (таких, як потік повідомлень), визначати автентичність джерела даних (іншими словами, того, хто є автором інформації), а також гарантувати неможливість відмовитися від зроблених дій («неспростовність»).

Як вказувалося, в основі криптографічного контролю цілісності лежать два поняття – хеш-функція та ЕЦП.

ЕЦП служить тієї ж меті, що печатка або власноручний підпис на паперовому документі. Однак внаслідок своєї цифрової природи ЕЦП перевершує ручний підпис і печатку в ряді дуже важливих аспектів. Цифровий підпис не тільки підтверджує особистість того, хто підписав, але також допомагає визначити, чи був зміст підписаної інформації змінений.

Власноручний підпис і печатка не мають подібної якості; крім того, їх набагато легше підробити.

Хеш-функція – це важкообратиме перетворення даних (однобічна функція), реалізоване, як правило, засобами симетричного шифрування зі зв'язуванням блоків. Результат шифрування останнього блоку (що залежить від всіх попередніх) і служить результатом хеш-функції.

Щоб зрозуміти, чому значення хеш-функції завжди має однакову довжину і не залежить від вихідного тексту, можна спрощено представити хеш-функцію у вигляді кодового замку з коліщатками. Спочатку ми виставляємо всі коліщатка в «нуль», потім йдемо по тексту і для кожної букви прокручуємо коліщатка відповідно до деяких правил. Те число, яке виявиться на замку в кінці, і є значенням хеш-функції.

Використання ЕЦП включає дві процедури:

1) процедуру постановки підпису відправником;

2) процедуру перевірки підпису отримувачем.

У процедурі постановки підпису використовується секретний ключ відправника повідомлення, в процедурі перевірки підпису – відкритий ключ відправника.

При формуванні ЕЦП відправник обчислює хеш-функцію *h(T)* текст, що підписується *T* (так званий дайджест). Обчисленим значенням *S* хеш-функції *h(T)* є один короткий блок інформації, що характеризує увесь текст *N* в цілому. Потім число *S* шифрується секретним ключем відправника. Отримана при цьому пара чисел й є ЕЦП для даного тексту N*M*.

При перевірці ЕЦП одержувач повідомлення знову обчислює хеш-функцію $m = h(T)$ прийнятого тексту *T*, після чого за допомогою відкритого ключа відправника перевіряє, чи відповідає отриманий підпис *S* обчисленому значенню хеш-функції.

На рис. 3.12 показана процедура вироблення та перевірки електронного цифрового підпису.

Процедура вироблення полягає в шифруванні перетворенням D дайджесту *h(T)*. При перевірці з рівності $E(S') = h(T')$ слідує, що $S' = D(h(T'))$ (для доказу досить застосувати до обох частин перетворення *D* і викреслити в лівій частині тотожне перетворення $D(E(T))$).

Перелік міжнародних та європейських стандартів, інших актів технічного регулювання системи електронного цифрового підпису визначений наказом Міністерства юстиції України, Адміністрації Державної служби спеціального зв'язку та захисту інформації України 05.12.2013 № 2563/5/645.

При використанні ЕЦП необхідно мати гарантію автентичності пари (ім'я користувача, відкритий ключ користувача). Для вирішення цього зав-

дання уводяться поняття *цифрового сертифіката й засвідчувального центра* (згідно з міжнародними специфікаціями X.509). Таким чином формується інфраструктура електронного цифрового підпису.

Засвідчувальний центр – це компонент глобальної служби каталогів, відповідальний за керування криптографічними ключами користувачів. Кореневим каталогом цієї служби є центральний засвідчувальний орган (ЦЗО).

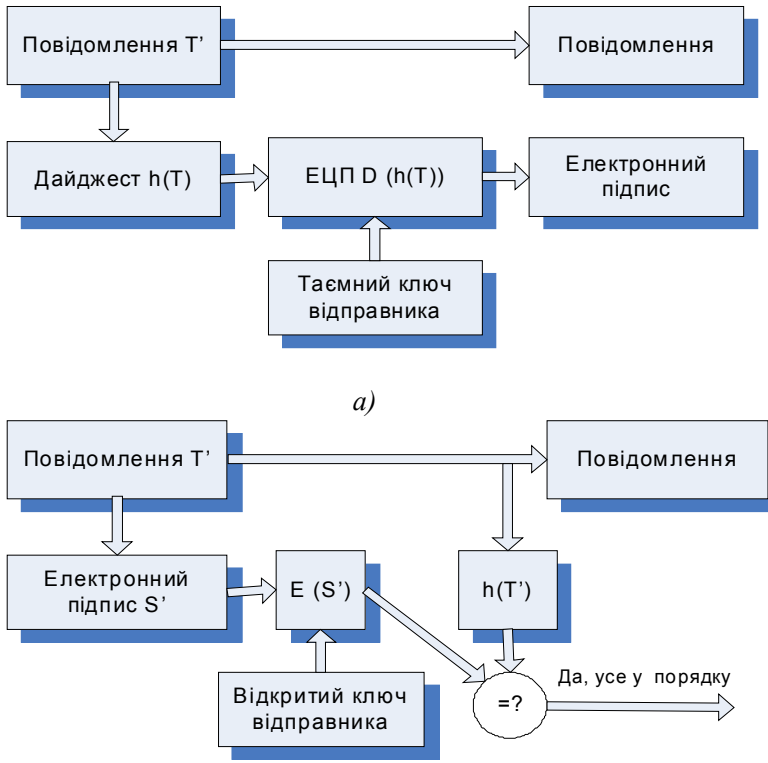


Рис. 3.12. Використання ЕЦП
(а – вироблення ЕЦП, б – його перевірка)

Відкриті ключі й інша інформація про користувачів реєструється і зберігається засвідчувальними центрами у вигляді *цифрових сертифікатів*, що мають наступну структуру:

- порядковий номер сертифіката;
- ідентифікатор алгоритму електронного підпису;

- ім'я засвідчувального центра;
- термін придатності;
- ім'я власника сертифіката (ім'я користувача, якому належить сертифікат);
- відкриті ключі власника сертифіката (ключів може бути кілька);
- ідентифікатори алгоритмів, асоційованих з відкритими ключами власника сертифіката;
- електронний підпис, згенерований з використанням секретного ключа засвідчувального центра (підписується результат хешуванням всієї інформації, що зберігається в сертифікаті).

Цифрові сертифікати у форматі X.509 стали не тільки формальним, але й фактичним стандартом, що підтримується численними засвідчувальними центрами. Це дозволило утворити інфраструктуру обігу електронних документів.

Контрольні запитання та завдання

1. Поясніть сучасну модель захисту інформації, що передається.
2. Чим у сучасних шифрах визначається стійкість шифру?
3. Чи можлива побудова абсолютно стійкого шифру?
4. Розгляньте загальну класифікацію алгоритмів шифрування та надайте пояснень по кожному елементу класифікації.
5. Зашифруйте своє ім'я з використанням шифру Цезаря кілька разів з різними ключами, наприклад, 3, 4, 5. 6, 7. Спробуйте винайти в отриманих шифротекстах спільні символи, що можуть допомогти у дешифруванні.
6. Використайте шифр Віженера для шифрування власного прізвища, змінюючи кодове слово або ключ. Оцініть різницю в отриманих шифоротекстах.
7. Поясніть особливість симетричних алгоритмів шифрування та пов'язаних з їх використанням проблем.
8. Охарактеризуйте криптографію з відкритим ключем, її переваги та недоліки.
9. Що таке хеш-функція і у чому її переваги для застосування для контролю цілісності текстів?
10. Поясніть схеми генерування те перевірки електронного цифрового підпису.
11. У чому полягає призначення цифрових сертифікатів?

3.5. АНТИВІРУСНИЙ ТА МЕРЕЖЕВИЙ ЗАХИСТ

Методи виявлення вірусів.
Типи антивірусних засобів.
Мережні засоби захисту.
Політика безпеки при використанні Інтернету

3.5.1. Методи виявлення вірусів антивірусними засобами

Сучасні СППР важко уявити без використання мережевих засобів, зокрема сервісів Інтернету. Інтернет є безпрецедентним і унікальним інформаційним ресурсом, який об'єднує в собі величезні об'єми інформації, потрібної для підтримки прийняття рішень в усіх сферах діяльності. Водночас Інтернет є й джерелом загроз для СППР, причому має місце поява усе нових та нових загроз та атак, які провадяться через Інтернет і носять комплексний характер, використовуючи різні вразливості серверів та комп'ютерів користувачів. Як вказувалося, такі атаки реалізуються, як правило, початковим інфікуванням багатьох сайтів, подальшим розміщенням на інфікованих серверах коду, який вражатиме комп'ютери користувачів і вже ці комп'ютери можуть стати площадками подальших атак (зокрема захоплення нових серверів).

Ефективною протидією цим загрозам є антивірусне ПЗ (АВПЗ). В комплексі заходів комп'ютерної безпеки антивірусна програма знаходиться на першому місці.

Сучасні антивірусні програми можуть знаходити оперативно десятки тисяч вірусів та видаляти їх. Якщо ж вірус видалити не вдається, то заражена програма знищується.

Антивірус – програма, призначена для захисту від вірусів, виявлення заражених програмних модулів і системних областей, а також відновлення вихідного стану заражених об'єктів.

АВПЗ зазвичай використовує два різних підходи для виконання своїх задач (рис. 3.13):

- фільтрація по репутації;
- знаходження підозрілої поведінки програм.

У міру того, як еволюціонували віруси, ускладнювалися й розвивалися технології їх детектування. Коротко ознайомимося з ними.

Рис. 3.13. Методи пошуку шкідливого коду антивірусними засобами

Найперша технологія пошуку шкідливих програм була заснована на *методі відповідності визначенню вірусів в словнику,* що полягає у перегляді (скануванні) файлів для пошуку ділянок коду відомих вірусів, так званих *сигнатур*, які однозначно ідентифікують ту або іншу шкідливу програму. У випадку відповідності ділянки коду відомому коду (сигнатурі) вірусу в словнику, програма-антивірус може виконувати одну з наступних дій:

- вилучити інфікований файл;
- відправити файл в карантин (тобто зробити його недоступним для виконання, з метою недопущення подальшого розповсюдження вірусу);
- намагатися відтворити файл (лікувати), видаливши сам вірус з тіла файлу.

Антивірусні програми, створені на основі пошуку відповідності визначенню вірусу в словнику, за звичайних обставин можуть досить ефективно перешкоджати випадкам зараження комп'ютерів. З 1990-х років автори вірусів, намагаючись триматися на крок-півкроку попереду програм-антивірусів, почали створювати «олігоморфні», «поліморфні» и, найновіші, «метаморфні» віруси, в яких декотрі частини тіла змінюються, шифруються або спотворюється так, щоб неможливо було знайти збіг з визначенням в словнику вірусів.

Для боротьби з вірусами, що маскуються, були розроблені додаткові спеціальні методи. Останнім часом з'явився і успішно розвивається новий антивірусний сегмент, який аналітики назвали STAP-Specialized Threat Analysis and Protection (спеціальні засоби аналізу і захисту). Для продуктів STAP характерне використання більшою мірою не сигнатур, а технологічних методик: пісочниць для попереднього завантаження даних, емуляції, аналізу великих даних, контейнеризації даних.

Так, наприклад, програми-антивіруси, що використовують *метод емуляції,* намагаються імітувати початок виконання коду кожної нової програми, що викликається для виконання, перед тим як передати їй керування. Якщо програма використовує код, що змінюється самостійно, або проявляє себе як вірус (тобто починає шукати інші exe-файли, наприклад), така програма буде вважатися шкідливою, здатною нашкодити іншим файлам. Однак цей метод має велику кількість помилкових попереджень.

Антивіруси, що використовують метод *знаходження підозрілої поведінки програм,* не намагаються ідентифікувати відомі віруси, замість цього вони відслідковують поведінку всіх програм. Якщо програма намагається записати якісь данні в файл, що виконується (exe-файл), програма-антивірус може зробити помітку цього файлу, попередити користувача і спитати, що треба зробити. що схожа на поведінку зараженої програми.

На відміну від методу відповідності визначенню вірусів в словнику, метод знаходження підозрілої поведінки дає захист від абсолютно нових вірусів, яких ще немає в жодному словнику вірусів. Однак треба враховувати, що програми, побудовані на цьому методі, видають також велику кількість помилкових попереджень.

Який би метод не застосовувався, у будь-якій захисній технології можна виділити дві компоненти: технічну і аналітичну. Ці компоненти не обов'язково чітко розмежовані на рівні модулів або алгоритмів, але на функціональному рівні вони помітні.

Технічна компонента – це сукупність програмних функцій і алгоритмів, що забезпечують аналітичний компонент даними для аналізу. У якості таких можуть виступати, приміром, байтовий код файлу, текстові рядки усередині файлу, одинична дія програми в рамках операційної системи або цілий ланцюжок таких дій.

Аналітична компонента – це система прийняття рішення. Це алгоритм, що аналізує наявні в його розпорядженні дані й виносить про них якесь судження. Відповідно до цього судження антивірус (або інше захисне ПЗ) вчиняє встановлені його політикою безпеки дії: сповіщає користувача, запитує в нього подальші вказівки, поміщає файл у карантин, блокує несанкціоновану дію програми й т.ін.

Складність алгоритму прийняття рішень аналітичною компонентою може бути будь-якою. Дуже умовно можна розділити аналітичні системи антивірусів на три категорії, між якими може бути безліч проміжних варіантів.

1. Просте порівняння. Вердикт виноситься за результатами порівняння єдиного об'єкта з наявним зразком. Результат порівняння бінарний («так» або «ні»).

2. Складне порівняння. Рішення приймається за результатами порівняння одного або декількох об'єктів з відповідними зразками. Шаблони для порівняння можуть бути гнучкими, а результат порівняння – імовірнісним.

3. Експертна система. Застосовується витончений аналіз даних, навіть з застосуванням методів штучного інтелекту, наприклад, методів машинного навчання.

3.5.2. Типи антивірусних засобів

Усю множину антивірусних програм можна умовно розділити на п'ять типів – фільтри, ревізори, детектори, доктори та імунізатори.

1. Програми-фільтри (вартові) – це резидентні програми, що контролюють дії, які відбуваються при роботі користувача на комп'ютері, та які можуть бути характерними для вірусних програм.

2. Програми-ревізори – це програми, що запам'ятовують початкові стани системних областей, каталогів і програм і періодично порівнюють поточні стани з початковими, прийнятими за еталонні.

3. Програми-детектори призначені просто для пошуку і виявлення вірусів в оперативній пам'яті і на машинних носіях. При виявленні підозрілого об'єкту видається відповідне повідомлення. Для нейтралізації виявленого вірусу необхідно скористатися якою-небудь іншою антивірусною програмою або ж спробувати видалити підозрілий об'єкт власноруч.

4. Програми-доктори (поліфаги) призначені для виявлення і знешкодження вірусів.

5. Програми-імунізатори (вакцини) призначені для відвертання зараження файлів яким-небудь одним, конкретним вірусом, або ж низкою відомих вірусів шляхом їх вакцинації. Ідея методу вакцинації полягає в модифікації об'єкту, що захищається, так, щоб це не відбивалося на його нормальному функціонуванні, і в той же час віруси сприймали його як вже заражений, і тому не намагалися інфікувати наново.

Може здатися цілком очевидним, що декілька встановлених антивірусів, що використовують різні методи, захистять комп'ютер надійніше. Проте, це твердження помилкове – більшість антивірусів визначають своїх «колег» як загрозу, що є причиною конфлікту і появи збоїв в системі.

Водночас дехто вважають, що антивірус є даремною програмою, яка марно пожирає системні ресурси. Це твердження є в корені невірним. Усе більше версій АВПЗ вже здатні працювати без участі користувача, тому їх діяльність є непомітною. Також деякі користувачі думають, що антивірус реагує на шкідливу програму тільки у тому випадку, коли вона вже встигла встановитися. Насправді це не зовсім вірно – сучасні програми можуть

знешкодити вірус на етапі копіювання або відкриття. І частота спрацьовування антивірусного захисту говорить про її ефективність.

Тому на сьогодні антивірусні засоби поставляються вже як *комплекси захисту*, а саме для захисту:

- комп'ютерів користувачів (робочих станцій);
- мережних серверів;
- поштових систем;
- мережних шлюзів.

В розподілених системах вони виступають як компоненти єдиного централізованого керованого комплексу антивірусного захисту.

АПВЗ працюють на комп'ютері майже безперервно, тому до них висуваються жорсткі вимоги стосовно того, щоб не заважати іншим програмам. Характеристики антивірусного засобу, на які впливають його компоненти, наведено у табл. 3.1.

На сьогодні у світі виробляється значна кількість антивірусних засобів. Серед них такі, як Avast! Internet Security, Dr.Web Security Space, Eset NOD32 Antivirus, Eset Smart Security, Kaspersky Anti-Virus, Kaspersky Internet Security, Microsoft Security Essentials, Norton Internet Security, Panda Cloud Antivirus та ін. Як же вибрати серед них найкращій засіб?

Таблиця 3.1

Характеристики антивірусного засобу, на які впливають його компоненти

№ з/п	Характеристики	Тлумачення характеристики
Технічна компонента		
1	навантаження на систему	частина процесорного часу й оперативної пам'яті, безперервно або періодично задіяних у забезпеченні захисту, що обмежують швидкодію системи
2	безпека	ступінь ризику, якому піддається операційна система й дані користувача в процесі ідентифікації потенційно шкідливого коду
3	захищеність	відображає уразливість технології, тобто те, наскільки шкідливий код може утруднити процес ідентифікації себе
Аналітична компонента		
4	проактивність	здатність технології виявляти нові, такі, що ще не попадали в руки фахівців шкідливі програми; як наслідок, залежна частота відновлення антивірусу
5	відсоток помилкових спрацьовувань	здатність технології помилково захоплювати нешкідливі програми
6	навантаження на користувача	ступінь участі користувача у процесі винесення вердикту – підтвердження або спростування «підозр» аналітичної системи

Питання це є дуже складним і неоднозначним. Так, наприклад, в рекламі антивірусних програм зазвичай вказують статистичні дані щодо де-

тектування загроз. Проте якщо один антивірус за однакових умов виявив 99 загроз, а другий усього лише 85, це зовсім не означає, що другий гірше. Один і той же файл цілком може визначатися по-різному. Саме ця причина і викликає розбіжність в статистиці визначення загроз різними засобами.

Щоб полегшити клієнтам вибір засобу, чимало аналітичних компаній постійно проводять тестування АВПЗ. Для оцінки вибирають різні групи критеріїв – від простих характеристик, на кшталт тих, що вказані в табл. 3.1, до випробування в найскладніших умовах – за відсутності оновлення антивірусних баз, доступу до хмарних сервісів, тощо.

Зазвичай як загальні критерії застосовуються уповільнення роботи системи при використанні антивірусу, зручність інтерфейсу, простота використання, функціональність, стійкість до збоїв, гнучкість настроювань, простота установки.

Для оцінки якості захисту враховуються швидкість реакції, якість сигнатурного детектування, якість евристичного аналізатора, якість поведінкового блокатора, можливість лікування активних заражень, можливість виявлення активних руткитів, самозахист, підтримка пакувальників, кількість помилкових спрацьовувань.

Іноді як еталон, з яким порівнюють результати протестованих антивірусів, використовують «ідеальний антивірус» з ергономічністю 100%. Під ним розуміється такий продукт, який виконує всі операції за мінімальний час, при роботі з яким не виникає помилок, який містить усі можливі засоби навчання і реалізує несуперечливу інформаційну модель.

3.5.3. Мережні засоби захисту

Інтернет, який став важливим ресурсом СППР та змінив стиль діяльності осіб, що приймають рішення, використовує для взаємодії стек протоколів TCP/IP (Transmission Control Protocol/Internet Protocol). Але фундаментальна проблема Інтернету полягає в тому, що при проектуванні він і не замислювався як захищена мережа. Серйозні і широко поширені проблеми з безпекою в Інтернеті пов'язані з уразливостями поточних версій TCP/IP, а саме:

- легкість перехоплення даних і фальсифікації адрес обладнання у мережі, адже основна частина трафіку Інтернету – це нешифровані дані, тому електронна пошта, паролі і файли можуть бути перехоплені, використовуючи легко доступні програми;
- низка засобів TCP/IP не захищені і можуть бути скомпрометованими кваліфікованими зловмисниками, особливо уразливі засоби, що використовуються для тестування;

- відсутність політики безпеки багатьох сайтів, які з-за незнання зконфігуровані таким чином, що надають широкий доступ до себе з боку Інтернету, і не намагаються обмежити доступ до інформації про свої комп'ютери, що може допомогти зловмисникам;
- складність конфігурування засобів керування доступом хостів, з-за чого важко правильно зконфігурувати і перевірити ефективність налаштувань.

Єдиним перспективним шляхом побудови спеціалізованих сервісів мережної безпеки, які допускають формальну або неформальну верифікацію, є використання комплексу засобів захисту, серед яких, поряд з антивірусними засобами та засобами контролю доступу важливе місце займають *міжмережні екрани, засоби виявлення та запобігання вторгнень, а також віртуальні приватні мережі* (рис. 3.14).

Рис. 3.14. Комплекс засобів і методів мережного захисту

Міжмережний екран, або **брандмауер** *(Firewall)* – програмно-апаратний комплекс засобів захисту локальної (корпоративної) мережі від несанкціонованого доступу ззовні (з Інтернету).

Засоби виявлення вторгнень *(IDS – Intrusion Detection system)* – програмно-апаратний комплекс сканування мережних засобів з метою виявлення небажаного трафіку.

Засоби запобігання вторгненням *(IPS – Intrusion Prevention system)* – програмно-апаратний комплекс засобів аналізу подій в системі з метою виявлення підозрілих.

Віртуальна приватна мережа *(VPN – Virtual Private Network)* – захищені тунелі між міжмережними екранами, накладені зазвичай поверх Інтернету.

Послідовність застосування вказаних засобів мережного захист «на підступах» до СППР з боку зовнішнього середовища показана на рис. 3.15.

Познайомимось поближче з цими засобами, і почнемо з міжмережних екранів (МЕ). Головна функція цих екранів – керування доступом до мережі, що захищається, шляхом фільтрування пакетів, що надходять до корпоративної мережі з Інтернету або направляються в Інтернет. Загальну схему екранування мережі показано на рис. 3.16.

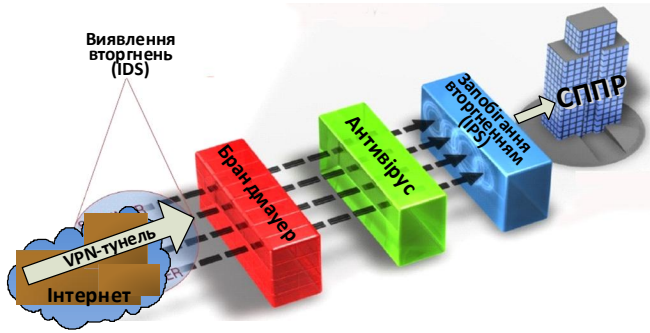


Рис. 3.15. Послідовність застосування засобів мережного захисту

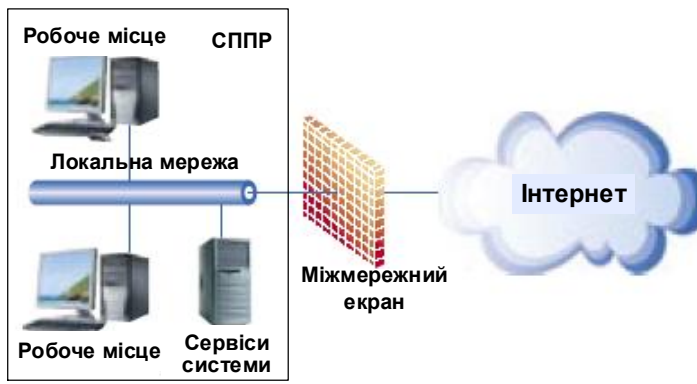


Рис. 3.16. Загальна схема екранування мережі

МЕ забезпечують декілька типів захисту:

- блокування небажаного трафіку;
- спрямовування вхідного трафіку тільки до надійних внутрішніх систем;
- приховування уразливих внутрішніх системи, яких не можна захистити від атак з Інтернету іншим засобом;

- протоколювання трафіку між внутрішньою мережею і Інтернетом;
- приховування службової інформації, такої як імена систем, топологія мережі, типи мережних пристроїв, внутрішні ідентифікатори користувачів, від Інтернету.

Екранування допомагає підтримувати доступність сервісів внутрішньої області, зменшуючи або взагалі ліквідуючи навантаження, викликане зовнішньою активністю. Зменшується уразливість внутрішніх сервісів безпеки, оскільки спочатку зловмисник повинен перебороти екран, де захисні механізми зконфігуровані особливо ретельно. Екранування дає можливість контролювати також інформаційні потоки, спрямовані в зовнішню область, що сприяє підтримці режиму конфіденційності в СППР.

В міжмережних екранах використовується модель *фільтрації*. МЕ зручно представляти як напівпроникну мембрану, реалізовану послідовністю фільтрів. Кожний з фільтрів, проаналізувавши дані, може затримати (не пропустити) їх, а може й відразу «перекинути» за екран. Крім того, допускається перетворення даних, передача порції даних на наступний фільтр для продовження аналізу або обробка даних від імені адресата й повернення результату відправникові (рис. 3.17).

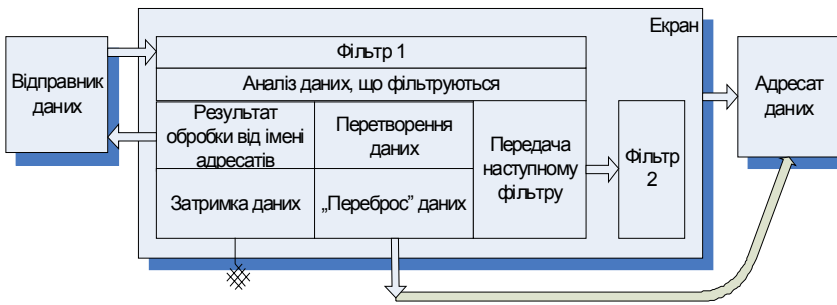


Рис. 3.17. Міжмережний екран як послідовність фільтрів

З точки зору користувача, МЕ – це захисна стіна, що стоїть між мережним адаптером та операційною системою. Будь-який IP-пакет, перш ніж потрапити на обробку ОС (наприклад, для маршрутизації або передачі його web-серверу) проходить через строгий контроль. Будь-який вихідний пакет також натрапляє на цю стіну, і може бути пропущений, відкинутий, підрахований або змінений. При складній обробці пакету він може проходити через брандмауер і більшу кількість разів.

Рішення про те, пропустити або затримати дані, приймаються для кожного пакета незалежно, на підставі аналізу адрес і інших полів заго-

ловків пакетів. Ще один важливий компонент – це порт, через який надійшов пакет.

Фільтрація інформаційних потоків здійснюється міжмережними екранами на основі *набору правил,* що відображають мережні аспекти політики безпеки. У цих правилах, крім інформації, яка утримується у потоках, що фільтруються, можуть фігурувати й інші дані, отримані з оточення, наприклад, поточний час, кількість активних з'єднань, порт, через який надійшов мережний запит, і т.ін.

Міжмережний екран – ідеальне місце для вбудовування засобів активного аудита. МЕ здатний реалізувати потужну реакцію на підозрілу активність, аж до розірвання зв'язку із зовнішнім середовищем.

На МЕ доцільно покласти ідентифікацію/автентифікацію зовнішніх користувачів, що потребують доступу до корпоративних ресурсів (з підтримкою концепції єдиного входу в мережу).

Існує дуже багато різних брандмауерів, кожний з яких забезпечує безпеку на тому чи іншому рівні, і у кожного з них є свої переваги та недоліки.

Всі міжмережні екрани можна поділити на три основних типи:

- пакетні фільтри (packet filter);
- шлюзи рівня з'єднання (circuit gateways);
- шлюзи прикладного рівня (application gateways).

Всі типи можуть одночасно зустрітися в одному брандмауері.

Пакетні фільтри ми щойно розглянули. Що стосується шлюзу рівня з'єднання, то це фактично транслятор TCP-з'єднання. Користувач встановлює з'єднання з певним портом на брандмауері, який провадить з'єднання з місцем призначення по інший від себе бік. Під час сеансу цей транслятор копіює байти в обох напрямках, діючи як провід. Як правило, пункт призначення задається заздалегідь, у той час як джерел може бути багато, тобто з'єднання типу «один – багато». Сферою застосування сервера рівня з'єднання може бути організація віртуальних приватних мереж.

Основним постачальником брандмауерів у світі є компанія Cisco, вироби якої завоювали популярність у тих, хто розробляє системи захисту.

Засоби виявлення вторгнень та запобігання вторгненням зазвичай поєднують у єдиний комплекс – систему IDS/IPS. Використання спеціальних автоматизованих засобів виявлення та попередження небажаних вторгнень є комплексним елементом таких видів робіт, що взаємно пересікаються, як атестація, моніторинг, аудит, і відносяться до так званих систем аналізу захищеності. Ці системи, що також мають назву скануюче програмне забезпечення (scanning software) або сканери безпеки (security

scanner), як і засоби активного аудиту, засновані на нагромадженні й використанні знань про прогалини в захисті – про те, як їх шукати, наскільки вони серйозні і як їх усувати. Серед таких сканерів найбільш ефективними є мережні сканери.

Система IDS/IPS складає «карту» мережі, що містить інформацію про потенційно слабо захищені місця, стан ОС, роботу додатків і протоколів, кількість і типи мережевих пристроїв (робоча станція, сервер, маршрутизатор) й ін. Маючи вичерпну інформацію про стан мережі в реальному часі, засоби IDS/IPS аналізують лише ті події, які можуть вплинути на безпеку системи, і не обробляють події, які ніяк на ній не позначаться.

Крім того, система IDS/IPS полегшує роботу адміністраторів безпеки за рахунок того, що може рекомендувати застосовувати ті або інші правила захисту від загроз, характерних для певного сімейства ОС, які використовуються в системі.

Серед лідерів ринку засобів IDS/IPS виділяються компанії Cisco, McAfee, Symantec та ін.

Розглядаючи такий важливий в сучасних умовах захисний засіб, як віртуальні приватних мережі (ВПМ), треба познайомитесь з таким самостійним сервісом безпеки як тунелювання (рис. 3.18).

Рис. 3.18. Захищена корпоративна мережа на базі ВПМ

Його суть полягає в тому, щоб «упакувати» передану порцію даних, разом зі службовими полями, у новий «конверт». Як синоніми терміна

«тунелювання» можуть використовуватися «конвертування» й «обгортання». Комбінація тунелювання й шифрування (поряд з необхідною криптографічною інфраструктурою) на виділених шлюзах і екранування власне й дозволяє реалізувати ВПМ. У ВПМ створюється закритий для сторонніх канал обміну інформацією. Це дозволяє об'єднати, наприклад, декілька віддалених мереж підприємства в єдину захищену корпоративну мережу щоб забезпечити користувачів СППР доступом до ресурсів системи (рис. 3.18). Кінцями тунелів, крім корпоративних міжмережних екранів, можуть бути мобільні комп'ютери користувачів (точніше, їх персональні МЕ).

3.5.4. Політика безпеки при використанні Інтернету

Незважаючи на те, що внутрішня зона СППР і зовнішнє середовище, як правило, розділяються за допомогою брандмауера, проте певні інтернетовські служби усе ж таки мають бути доступними внутрішнім користувачам, адже Інтернет стає усе більш важливим для виконання повсякденної ділової діяльності. Наприклад, таким зазвичай потрібним сервісом є електронна пошта. Крім того, система може мати власний інформаційний сайт в Інтернеті.

Для забезпечення безпеки у таких обставинах шляхом зменшення числа уразливих місць і, як наслідок, зменшення ризику, необхідно впроваджувати політику безпеки при використанні Інтернету. Для того, щоб розробити ефективну і недорогу в реалізації політику безпеки для захисту з'єднань з Інтернетом, потрібно виконати певний аналіз ризику для оцінки рівня жорсткості політики, що визначить необхідні витрати на засоби забезпечення безпеки для виконання вимог політики. Те, наскільки жорсткої буде політика, залежить від рівня загроз, яким піддається система і видимості ресурсів системи з зовнішнього світу, уразливості системи щодо потенційних інцидентів із безпекою, та нормативного забезпечення – державних законів, вимог вищестоящих організацій, що можуть явно диктувати застосування конкретних засобів та методів забезпечення безпеки для конкретних систем, додатків або видів інформації.

Для того щоб розробити ефективну політику безпеки, інформація, що обробляється в СППР, повинна бути класифікованою відповідно до її критичності до втрати конфіденційності, доступності або цілісності. На основі цієї класифікації потім можна легко розробити політику для дозволу (або заборони) доступу до Інтернету або для приймання інформації з Інтернету.

До засобів забезпечення безпеки з'єднання з Інтернетом усе частіше висуваються вимоги безперервності роботи, так званої високої доступ-

ності. Ці вимоги часто дуже впливають на політику безпеки, вимагаючи компромісних рішень. Передусім це стосується брандмауера, який може виявитися критичним місцем – якщо він вийде з ладу, зв'язок з Інтернетом може виявитися неможливим на час усунення аварії. Якщо тимчасова втрата зв'язку з Інтернетом не робить великого впливу на функціонування системи, політика може просто визначати, що робота з Інтернетом припиняється доти, поки не буде відновлений брандмауер. Проте, якщо використання Інтернету є необхідним, і при цьому інформація має високий рівень ризику, політика може вимагати використання брандмауера з резервом (гарячим або холодним). Аналогічно подібна надлишковість може бути потрібною й для серверів автентифікації або серверів віддаленого доступу, тобто наявності можливості швидко переключатися на резервний сервер. Головне питання при використанні резервних засобів – це синхронізація. Усі відновлення, резервні копії і модифікації повинні провадитися на обох пристроях.

Крім надлишковості обладнання основними заходами задоволення вимог високої доступності є планування ресурсів та заходи відновлення обладнання після аварій. Детальне планування виділення ресурсів важливе тому, що засоби безпеки, які суттєво зменшують продуктивність роботи системи, будуть швидко відключатися. У разі відновлення блоку, що вийшов з ладу, має здійснюватися ретельний контроль його конфігурації після відновлення, щоб гарантувати, що працюють усі необхідні продукти, їхні версії актуальні, і до них застосовані всі модифікації і виправлення.

При організації з'єднань через Інтернет низку проблем має ідентифікація та автентифікація. Зловмиснику достатньо легко можна перехопити дані авторизації і повторити їх, щоб видати себе за легального користувача. Безпека традиційних схем з використанням паролів в основному залежить від складності угадування паролів і того, наскільки добре вони захищені.

Для забезпечення підвищеної безпеки застосовується так звана стійка автентифікація, що використовує криптографію або інші засоби для створення одноразових паролів. Цей клас автентифікації використовує динамічні дані, що змінюються з кожним сеансом автентифікації. Одним із засобів реалізації цього є опрацювання за допомогою алгоритму генерації електронних підписів кожного біта даних, що посилаються від користувача до серверу при автентифікації.

Які б засоби не застосовувались, необхідно дотримуватись загальних правил використання паролів при автентифікації в Інтернеті, а саме:

- ідентифікатори користувачів і їх паролі повинні бути унікальними для кожного користувача;

- паролі повинні складатися як мінімум із 8 символів, триматися в таємниці, не повинні вставляться в тексти програм та ін.;
- у системі спеціальними програмами повинне провадитися періодичне тестування на предмет виявлення паролів, що вгадуються;
- паролі повинні періодично змінюватися, а в системі можуть застосовуватися засоби, що змушують користувача примусово поміняти пароль через визначений час і запобігти використанню того ж самого або пароля, що вгадується;
- акаунти користувачів повинні бути заблоковані після 3 невдалих спроб входу в систему або після визначеного часу відсутності використання, а всі випадки невірно введених паролів повинні бути записані в системний журнал;
- сеанси користувачів із сервером повинні блокуватися після певного періоду неактивності, а для відновлення сеансу має знову вимагатися уведення пароля.

Важливим розділом політики безпеки в Інтернеті є політика щодо вірусів. Передусім треба виходити з того, що будь-яка зміна даних або програм на комп'ютерах несе в собі ризик зараження вірусами. При імпорті програм на комп'ютері і їхньому запуску на ньому є ризик, що ці програми мають додаткову функціональність або їхні реальні функції відрізняються від заявлених. Прикладами явного імпорту є:

- передача файлів – використання FTP для переносу файлу на комп'ютер.
- читання електронної пошти – читання повідомлення, завантаженого на комп'ютер, або використання зовнішньої програми (наприклад, MS Word) для читання додатків до листа;
- завантаження програм з Інтернету.

Політика безпеки для боротьби з вірусами повинна мати три складові частини:

- запобігання – правила, що дозволяють запобігти зараженню вірусами;
- виявлення – як визначити, що даний виконуваний файл, завантажувальний запис, або файл даних має вірус;
- вилучення – як вилучити вірус з зараженої комп'ютерної системи (це може потребувати переінсталяції ОС, вилучення файлів, або вилучення вірусу з зараженого файлу).

Для забезпечення виявлення повинні проводитись щоденні перевірки на віруси й використовуватися комерційні антивірусні програми. Антивірусні програми повинні обновлятися згідно із встановленим виробником періодом. Перевірка усіх файлових систем повинна провадитися щодня

в обов'язковому порядку. Результати перевірок повинні протоколюватися, автоматично збиратися й аналізуватися системними адміністраторами та адміністраторами безпеки.

Для користувачів має бути запровадженою програма навчання комп'ютерної безпеки, що повинна містити інформацію про ризик зараження вірусами та необхідні дії користувачів.

Контрольні запитання та завдання

1. Які два підходи для виконання своїх задач зазвичай використовують антивірусні засоби та в чому полягають відмінності між ними?

2. Поясніть суть роботи програм-антивірусів, що використовують метод емуляції.

3. Які дві основні компоненти можна виділити у будь-якій захисній антивірусній технології та у чому їх сутність?

4. На які категорії можна розділити аналітичні системи антивірусів?

5. На які типи можна умовно розділити множину антивірусних програм?

6. У вигляді яких компонентів виступає єдиний централізований комплекс антивірусного захисту в розподілених системах?

7. Назвіть характеристики антивірусного засобу, на які впливають його компоненти.

8. Які критерії застосовуються для оцінки антивірусних програм при їх тестуванні?

9. Які засоби складають комплекс захисту у мережному середовищі?

10. У чому полягає головна функція міжмережних екранів?

11. Поясніть принцип моделі фільтрації, що використовується в міжмережних екранах.

12. Для чого використовують засоби виявлення вторгнень та запобігання вторгненням?

13. Що таке віртуальні приватних мережі та на чому вони базуються?

14. Для чого впроваджується політика безпеки при використанні Інтернету?

15. Охарактеризуйте розділ політики безпеки в Інтернеті присвячений захисту від вірусів.

ЛІТЕРАТУРА

1. *Антонюк А.О.* Основи захисту інформації в автоматизованих системах: навч. посібн. / А.О. Антонюк – К.: Видавн. дім «КМ Академія», 2003. – 244 с.
2. *Будько М.М.* Вільне програмне забезпечення: український вибір / М.М. Будько, О.В. Нестеренко, І.Є. Нетесін. – К.: Альтерпрес, 2011. – 400 с.
3. *Гайворонський М.В.* Безпека інформаційно-комунікаційних систем: підручн. / М.В. Гайворонський, О.М. Новіков. – К.: Видавнича група BHV, 2009. – 608 с.
4. *Горбулін В.П.* Засади національної безпеки України: підручн. / В.П. Горбулін, А.Б. Качинський. – К.: Інтертехнологія, 2009. – 272 с.
5. *Жора В.* Підхід до моделювання ролевої політики безпеки / В. Жора // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, 2003. – Вип. 7. – С. 45-49.
6. *Нестеренко О.В.* Безпека інформаційного простору державної влади. Технологічні основи / О.В. Нестеренко. – К.: Наук. думка, 2009. – 352 с.
7. *Нестеренко О.В.* Інтелектуальні системи підтримки прийняття рішень: навч. посіб. / О.В. Нестеренко, О.І. Савенков, О.О. Фаловський. [За ред. Бідюка П.І.]. – К: Національна академія управління, 2016. – 188 с.
8. *Андрианов В.И.* Охранные системы для дома и офиса / В.И.Андрианов, А.В. Соколов. – СПб.: БХВ-Петербург; Арлит, 2002. – 304 с.
9. *Анин Б. Ю.* Защита компьютерной информации / Б. Ю. Анин – СПб.: БХВ-Санкт-Петербург, 2000. – 384 с.
10. *Галатенко В.А.* Основы информационной безопасности / В. А. Галатенко. Интернет-университет информационных технологий. – ИНТУИТ.ру, 2005.
11. *Герасименко В. А.* Основы защиты информации / В. А. Герасименко, А. А. Малюк. – М.: МОПО РФ – МГИФИ, 1997. – 538 с.
12. *Грушо А.А.* Теоретические основы защиты информации / А.А. Грушо, Е.Е. Тимонина. – М.: Яхтсмен, 1996. – 302с.
13. *Домарев В. В.* Безопасность информационных технологий. Системный поход / В. В. Домарев. – К.; М.; СПб.: Торгово-издательский дом «DiaSoft», 2004. – 975 с.

14. *Жельников В.* Криптография от папируса до комп'ютера / В. Жельников – М.: ABF, 1997. – 336 с.
15. *Медведовский И.* Аспекты защиты. Атака из Интернет / И. Медведовский, Б. Семьянов, Д. Леонов, А. Лукацкий. – М.: Солон-Р, 2002. – 368 с.
16. *Мельников В. В.* Безопасность информации в автоматизированных системах / В. В. Мельников. – М.: Финансы и статистика, 2003. – 368 с.
17. *Петраков А. В.* Основы практической защиты информации: Учебн. Пособие / А. В. Петраков. – 2-е изд. – М.: Радио и связь, 2000. – 368 с.
18. *Рублинецкий В.И.* Введение в компъютерную криптологию / В.И. Рублинецкий. – Харьков: ОКО, 1997.
19. *Стенг Дэвид.* Секреты безопасности сетей / Дэвид Стенг, Сильвия Муи. – К.: «Диалектика», Информейшн Компьютер Энтерпрайз, 1996. – 544 с.
20. *Торокин А.А.* Основы инженерно-технической защиты информации / А. А. Торокин. – М.: Ось-89, 1998. – 336 с.
21. *Шнайер Б.* Прикладная криптография: Протоколы, алгоритмы, исходные тексты на языке Си / Б. Шнайер. – М.: «Триумф», 2002. – 475 с.
22. *Шнайер Б.* Практическая криптография / Б. Шнайер, Н. Фергюссон. – К.: «Диалектика», 2006. – 575 с.
23. *Ярочкин В.И.* Информационная безопасность: Учебник для студентов вузов / В.И. Ярочкин. – М.: Академический Проект; фонд «Мир», 2003. – 640 с.

ПРЕДМЕТНИЙ ПОКАЖЧИК

А

Б

В

Г

Д

Е

Ж

З

І

К

Л

М

Н

О

П

Р

С

Т

У

Ф

Х

Ц

Ш

Навчальне видання

Ковтунець Володимир Вітальович
Нестеренко Олександр Васильович
Савенков Олександр Іванович

БЕЗПЕКА СИСТЕМ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ

Навчальний посібник

Відповідальний технічний редактор
та комп'ютерна верстка *Цаплюк І.В.*

Підп. до друку 13.09.2016. Формат 60x84/16
Папір офс. Гарнітура Times New Roman. Друк офс.
Ум. друк. арк. 10,80. Обл.-вид. арк. 8,97.
Тираж 300 прим. Зам. 36.

Національна академія управління
01011, м. Київ, вул. Вінницька, 10, км. 410.
тел. 246-24-45, 246-24-44, 280-80-56
www.nam.kiev.ua, eco@nam.kiev.ua, NAU-kniga@ukr.net

Віддруковано в типографії
ТОВ "Наш формат", 02105,
м. Київ, пр-т Миру, 7