БЕЗПЕКА ЕКОНОМІЧНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

1. Інформаційна безпека комп'ютерних систем

1.1. Основні поняття та визначення

По мірі розвитку і ускладення засобів, методів та форм автоматизації процесів обробки інформації збільшується залежність суспільства від безпеки використовуваних інформаційних технологій. Актуальність і важливість проблеми забезпечення безпеки інформаційних технологій обумовлені рядом причин [i]:

- різке збільшення обчислювальної потужності сучасних комп'ютерів при одночасному спрощенні їх експлуатації;
- різке збільшення об'ємів інформації, що накопичується, зберігається та обробляється за допомогою комп'ютерів та інших засобів автоматизації;
- накопичення в єдиних базах даних інформації різного призначення та різної належності;
- високі темпи росту кількості персональних комп'ютерів, що використовуються в найрізноманітніших сферах діяльності;
- різке розширення кола користувачів, що мають безпосередній доступ до обчислювальних ресурсів та масивів даних;
- стрімкий розвиток програмних засобів, що не задовольняють навіть мінімальним вимогам безпеки;
- повсюдне розповсюдження мережних технологій та об'єднання локальних мереж у глобальні;
- розвиток глобальної мережі Інтернет, яка практично не перешкоджає порушенням безпеки систем обробки інформації в усьому світі.

Введемо та визначимо основні поняття безпеки інформаційних систем [ii].

> Під ***безпекою*** інформаційної системи розуміють її захищеність від випадкового чи зловмисного втручання в нормальний процес її функціонування, а також від спроб викрадання, зміни чи знищення її компонентів.

Природа впливу на інформаційну систему може бути дуже різноманітною – стихійні лиха, вихід з ладу складових елементів ІС, помилки персоналу, спроба проникнення зловмисника тощо. Безпека ІС досягається прийняттям заходів із забезпечення конфіденційності та цілісності інформації, що обробляється нею, а також доступності і цілісності компонентів і ресурсів системи.

Під ***доступом до інформації*** розуміється ознайомлення з інформацією, її

обробка, зокрема копіювання, модифікація чи знищення інформації. Розрізняють санкціонований та несанкціонований доступ до інформації. ***Санкціонований доступ до інформації*** – це доступ до інформації, який не порушує встановлені правила розмежування доступу. ***Правила розмежування доступу*** служать для регламентації права доступу суб'єктів доступу до об'єктів доступу. ***Несанкціонований доступ до інформації*** характеризується порушенням встановлених правил розмежування доступу. Особа чи процес, що здійснюють несанкціонований доступ до інформації, є порушниками правил розмежування доступу. Несанкціонований доступ є найрозповсюдженішим видом комп'ютерних порушень.

Конфіденційність даних – це статус, який надається даним і який визначає необхідну міру їх захисту. По суті, конфіденційність інформації – це властивість інформації бути відомою тільки допущеним і авторизованим суб'єктам системи (користувачам, процесам, програмам). Для усіх інших суб'єктів системи ця інформація повинна бути невідомою. ***Суб'єкт*** – це активний компонент системи, який може стати причиною потоку інформації від об'єкта до суб'єкта чи зміни стану системи. ***Об'єкт*** – пасивний компонент системи, який зберігає, приймає чи передає інформацію. Доступ до об'єкту означає доступ до інформації, що в ньому міститься.

Цілісність інформації забезпечується в тому випадку, якщо дані в системі не відрізняються в семантичному відношенні від даних у вихідних документах – якщо не відбулося їх випадкового чи зумисного спотворення чи пошкодження. ***Цілісність*** компоненту чи ресурсу системи – це властивість компоненту чи ресурсу бути незмінним в семантичному змісті при функціонуванні системи в умовах випадкових чи зловмисних спотворень або руйнівних впливів. ***Доступність*** компоненту чи ресурсу системи – це властивість компоненту чи ресурсу бути доступним для авторизованих законних суб'єктів системи.

Під ***загрозою безпеці*** інформаційної системи розуміють можливі впливи на ІС, які прямо чи опосередковано можуть нанести шкоду її безпеці. ***Порушення безпеки*** передбачає порушення стану захищеності інформації, що міститься та обробляється в ІС. З поняттям загрози безпеці тісно пов'язане поняття вразливості ІС. ***Вразливість*** інформаційної системи – це деяка невдала властивість системи, яка робить можливим виникнення та реалізацію загрози.

Атака (***напад***) на комп'ютерну систему – це дія зловмисника, яка полягає в пошуку та використанні тієї чи іншої вразливості системи. Таким чином атака – це реалізація загрози безпеці.

Безпечна чи ***захищена система*** – це система із засобами захисту, які успішно і ефективно протидіють загрозам безпеки. ***Комплекс засобів захисту*** представляє собою сукупність програмних та технічних засобів, які створюються та підтримуються для забезпечення інформаційної безпеки ІС. Комплекс створюється та підтримується відповідно до прийнятої в даній організації політики безпеки. ***Політика безпеки*** – це сукупність норм, правил та практичних рекомендацій, що регламентують роботу засобів захисту ІС від заданої множини загроз безпеки.

1.2. Основні загрози безпеці інформаційних систем

За метою впливу розрізняють три основні типи загроз безпеці інформаційних систем [iii]:

- загрози порушення конфіденційності інформації;
- загрози порушення цілісності інформації;
- загрози порушення працездатності системи (відмови в обслуговуванні).

Загрози порушення конфіденційності направлені на розголошення конфіденційної чи секретної інформації. При реалізації цих загроз інформація стає відомою особам, які не повинні мати до неї доступ. В термінах комп'ютерної безпеки загроза порушення конфіденційності проявляється щоразу, коли отримано несанкціонований доступ до деякої закритої інформації, що зберігається в комп'ютерній системі чи передається від однієї комп'ютерної системи до іншої.

Загрози порушення цілісності інформації, що зберігається в комп'ютерній системі чи передається по каналу зв'язку, направлені на її зміну чи спотворення, що приводить до порушення її якості чи повного знищення. Цілісність інформації може бути порушена спеціально зловмисноком, а також в результаті впливу зовнішнього середовища, що оточує систему. Ця загроза є особливо актуальна для систем передачі інформації – комп'ютерних мереж та систем телекомунікацій. Зумисні порушення цілісності інформації не слід плутати з її санкціонованою зміною, яка здійснюється повноважними особами з обґрунтованою метою.

Загрози порушення працездатності (відмова в обслуговуванні) направлені на створення таких ситуацій, коли певні навмисні дії або знижують працездатність ІС, або блокують доступ до її ресурсів. Наприклад, якщо один користувач системи робить спробу отримати доступ до деякої служби, а інший здійснює дії з блокування цього доступу, то перший користувач отримує

відмову в обслуговуванні. Блокування доступу до ресурсу може бути постійним чи тимчасовим.

Порушення конфіденційності та цілісності інформації, а також доступності і цілісності певних ресурсів ІС можуть бути викликані різними небезпечними впливами на інформаційну систему. Сучасні автоматизовані системи обробки інформації представляють собою складну систему, що складається з великої кількості компонент різного ступеня автономності, які зв'язані між собою та обмінюються даними. Практично кожний компонент може піддаватися зовнішньому впливу чи вийти з ладу. Компоненти інформаційної системи можна розділити на такі групи:

- апаратні засоби;
- програмне забезпечення;
- дані;
- персонал

Небезпечні впливи на ІС можна поділити на випадкові та зловмисні. Аналіз досвіду проектування, виготовлення та експлуатації інформаційних систем показує, що інформація піддається різним випадковим впливам на всіх етапах функціонування інформаційної системи. Причинами випадкових впливів можуть бути:

- аварійні ситуації, пов'язані зі стихійними лихами та відключеннями електричного живлення;
- відмови та збої апаратури;
- помилки в програмному забезпеченні;
- помилки в роботі обслуговуючого персоналу та користувачів;
- завади в лініях зв'язку, спричинені впливом зовнішнього середовища.

Навмисні загрози пов'язані з цілеспрямованими діями порушника. Порушником може бути співробітник, відвідувач, конкурент, найманець тощо. Дії порушника можуть бути зумовлені різними мотивами: невдоволенням співробітника своєю кар'єрою, матеріальною зацікавленістю, цікавістю, конкурентною боротьбою, прагненням самоствердження та ін. Виходячи з можливості виникнення найнебезпечнішої ситуації, зумовленої діями порушника, можна скласти гіпотетичну модель потенційного порушника:

- кваліфікація порушника може бути на рівні розробника даної системи;
- порушником може бути як стороння особа, так і законний користувач системи;
- порушнику відома інформація про принципи роботи системи;
- порушник вибирає найслабшу ланку в захисті.

Можна виділити такі приклади навмисних загроз [iv]:

- несанкціонований доступ сторонніх осіб, що не належать до числа співробітників, та ознайомлення з конфіденційною інформацією;
- ознайомлення співробітників з інформацією, до якої вони не повинні мати доступ;
- несанкціоноване копіювання програм і даних;
- викрадення носіїв інформації, що містять конфіденційну інформацію;
- викрадення роздрукованих документів;
- навмисне знищення інформації;
- несанкціонована модифікація співробітниками фінансових документів, звітності та баз даних;
- фальсифікація повідомлень, що передаються по каналах зв'язку;
- відмова від авторства повідомлення, переданого каналом зв'язку;
- відмова від факту отримання інформації;
- пошкодження інформації, викликане впливом вірусів;
- пошкодження архівної інформації, розміщеної на змінних носіях;
- викрадення обладнання.

Несанкціонований доступ є найбільш розповсюдженим та різностороннім видом комп'ютерних порушень. Суть несанкціонованого доступу полягає в отриманні користувачем (порушником) доступу до об'єкту з порушенням правил розмежування доступу, встановлених у відповідності до прийнятої в організації політики безпеки [iv]. Несанкціонований доступ використовує будь-яку помилку в системі захисту та можливий при нераціональному виборі засобів захисту, некоректному їх встановленні та настроюванні. Несанкціонований доступ може бути здійснений як штатними засобами ІС, так і спеціально створеними апаратними і програмними засобами.

Наведемо перелік основних каналів несанкціонованого доступу, через які зловмисник може отримати доступ до компонентів ІС та здійснити крадіжку, модифікацію і/або пошкодження інформації:

- усі штатні канали доступу до інформації (комп'ютери користувачів, оператора, адміністратора системи; засоби відображення та документування інформації; канали зв'язку) при їх використанні порушниками, а також законними користувачами за межами їх повноважень;
- технологічні пульти управління;
- лінії зв'язку між апаратними засобами ІС;
- побічні електромагнітні випромінювання від апаратури, ліній зв'язку, мереж електричного живлення, заземлення тощо.

Із всього розмаїття способів та прийомів несанкціонованого доступу зупинимося на найбільш розповсюджених та зв'язаних між собою порушеннях:

- перехоплення паролів;
- „маскарад";
- незаконне використання привілеїв.

Перехоплення паролів здійснюється спеціально розробленими програмами. При спробі законного користувача ввійти в систему програма-перехоплювач імітує на екрані введення логіну та паролю користувача, які пересилаються власнику програми-перехоплювача після чого на екран виводиться повідомлення про помилку і управління повертається операційній системі. Користувач вважає, що допустив помилку при введенні паролю. Він повторює введення і отримує доступ в систему. Власник програми-перехоплювача, отримавши логін та пароль законного власника, може тепер їх використовувати в своїх цілях. Існують й інші способи перехоплення паролів.

„Маскарад“ – це виконання якихось дій одним користувачем від імені іншого, що має відповідні повноваження. Метою „маскараду“ є приписування якихось дій іншому користувачу або присвоєння повноважень та привілеїв іншого користувача. Прикладами реалізації „маскараду“ є:

- вхід в систему під іменем та паролем іншого користувача (такому „маскараду“ передує перехоплення паролю);
- передача повідомлень в мережі від імені іншого користувача.

„Маскарад“ є особливо небезпечним в банківських системах електронних платежів, де неправильна ідентифікація клієнта із-за „маскараду“ зловмисника може привести до великих втрат законного клієнта банку.

Незаконне використання привілеїв. Більшість систем захисту встановлюють певні набори привілеїв для виконання заданих функцій. Кожний користувач отримує свій набір привілеїв: звичайні користувачі – мінімальний, адміністратори – максимальний. Несанкціоноване захоплення привілеїв, наприклад засобами „маскараду“, приводить до можливості виконання порушником певних дій в обхід системи захисту. Слід зазначити, що незаконне захоплення привілеїв можливе або за наявності помилок в системі захисту, або із-за халатності адміністратора при управлінні системою та призначенні привілеїв.

Окремо слід зупинитися на загрозах, яким можуть піддаватися комп’ютерні мережі. Основна особливість будь-якої комп’ютерної мережі полягає в тому, що її компоненти розподілені в просторі. При вторгненні в комп’ютерну мережу зловмисник може використовувати як пасивні, так і активні методи вторгнення. При ***пасивному вторгненні*** (перехопленні інформації) порушник тільки спостерігає за проходженням інформації по каналу зв’язку, не втручаючись ні в інформаційний потік, ні в зміст інформації. Як правило, зловмисник може визначити пункти призначення та ідентифікатори або тільки факт проходження повідомлення, його довжину та частоту обміну, якщо зміст повідомлення розпізнати неможливо, – виконати аналіз трафіку (потоку повідомлень) в даному каналі.

При ***активному вторгненні*** порушник прагне підмінити інформацію, що передається в повідомленні. Він може вибірково модифікувати чи змінювати повідомлення, затримувати чи змінювати порядок слідування повідомлень. Зловмисник може також анулювати і затримувати усі повідомлення, що передаються по каналу. Такі дії можна кваліфікувати як відмову в передачі повідомлень.

Комп'ютерні мережі характерні тим, що крім звичайних локальних атак, які здійснюються в межах однієї системи, проти об'єктів мереж здійснюють так звані, ***віддалені атаки***. Зловмисник може перебувати за тисячі кілометрів від атакованого об'єкта, при цьому нападу може піддаватися не тільки конкретний комп'ютер, а й інформація, що передаються по мережним каналам зв'язку. Під віддаленою атакою розуміють інформаційний зловмисний вплив на розподілену комп'ютерну мережу, який здійснюється програмно з використанням каналів зв'язку [iv].

У табл. 1 показані основні шляхи реалізації загроз безпеці ІС при впливі на її компоненти. Ця таблиця дає тільки загальну картину того, що може відбутися з системою, а конкретні обставини та особливості повинні розглядатися окремо.

Таблиця 1.

Шляхи реалізації загроз безпеці ІС

Об'єкти впливу	**Порушення конфіденційності інформації**	**Порушення цілісності інформації**	**Порушення працездатності системи**
Апаратні засоби	Несанкціонований доступ – підключення; використання ресурсів; викрадення носіїв	Несанкціонований доступ – підключення; використання ресурсів; модифікація, зміна режимів	Несанкціонований доступ – зміна режимів; виведення з ладу; пошкодження
Програмне забезпечення	Несанкціонований доступ – копіювання; викрадення; перехоплення	Несанкціонований доступ – впровадження „троянських коней", „вірусів", „черв'яків"	Несанкціонований доступ – спотворення; знищення; підміна
Дані	Несанкціонований доступ – копіювання; викрадення; перехоплення	Несанкціонований доступ – спотворення; модифікація	Несанкціонований доступ – спотворення; знищення; підміна
Персонал	Розголошення; передача відомостей про захист; халатність	„Маскарад"; вербування; підкуп персоналу	Покидання робочого місця; фізичне усунення

У табл. 1 наведено специфічні назви та терміни: „троянський кінь“, „вірус“, „черв’як“. Хоча ці назви мають жаргонний відтінок, вони уже ввійшли в загальноприйнятий комп’ютерний лексикон. Дамо коротку характеристику цих розповсюджених загроз безпеці ІС.

„Троянський кінь“ представляє собою програму, яка поряд з діями, описаними в її документації, виконує деякі інші дії, що ведуть до порушення безпеки системи та деструктивних результатів. Аналогія такої програми з давньогрецьким „троянським конем“ повністю виправдана, оскільки в обидвох випадках оболонка, що не викликає підозр, містить в собі серйозну загрозу. Термін „троянський кінь“ було вперше використано Даном Едвардсом, який пізніше став співробітником Агенства Національної Безпеки США. „Троянський кінь“ використовує обман для того, щоб змустити користувача запустити програму з прихованою загрозою всередині. Зазвичай для цього стверджується, що така програма виконує деякі корисні функції. Зокрема, такі програми маскуються під якісь корисні утиліти.

Небезпека „троянського коня“ полягає в додатковому блоці команд, вбудованому у вихідну корисну програму, яка потім надається користувачам. Цей блок команд може спрацьовувати при настанні якоїсь умови (дати, стану системи) або по команді ззовні. Користувач, який запустив таку програму, піддає небезпеці як свої ресурси, так і всю ІС в цілому. Наведемо для прикладу деякі деструктивні функції, що реалізуються „троянськими конями“ [v]:

- ***знищення інформації***. Вибір об’єктів та способів знищення визначається фантазією та цілями автора зловмисної програми;
- ***перехоплення та передача інформації.*** Зокрема, відомі програми, які здійснюють перехоплення паролів, що набираються на клавіатурі;
- ***цілеспрямована модифікація тексту програми,*** яка реалізує функції безпеки та захисту системи.

Загалом, „троянські коні“ завдають збитки ІС шляхом викрадення інформації та явного пошкодження програмного забезпечення системи. „Троянський кінь“ є однією з найнебезпечніших загроз безпеці ІС. Радикальний спосіб захисту від цієї загрози полягає у створенні замкнутого середовища виконання програм, які повинні зберігатися і захищатися від несанкціонованого доступу. При цьому встановлення нового програмного забезпечення на комп’ютер повинно бути дозволено тільки адміністраторам, чого зазвичай складно досягти.

Комп’ютерні „віруси“ – це певний тип програмних об’єктів, які володіють рядом властивостей, притаманних живим організмам, – вони народжуються, розмножуються та помирають. Термін „вірус“ стосовно до

комп'ютерів був запропонований Фредом Коеном із Університету Південної Каліфорнії. Історично перше визначення, дане Ф. Коеном звучало так: „***Комп'ютерний вірус*** – це програма, яка може заражати інші програми, змінюючи їх шляхом включення в них своєї, можливо, зміненої копії, причому остання зберігає здатність до подальшого розмноження“ [vi]. Ключовими поняттями у визначенні комп'ютерного вірусу є здатність вірусу до саморозмноження та модифікації коду заражених програм.

Мережний „черв'як“ представляє собою різновид програми-вірусу, яка розповсюджується глобальною мережею і не залишає своєї копії на магнітному носії (хоча є й інші варіанти „черв'яків“, які зберігаються на фізичних носіях у вигляді файлів). Перші варіанти „черв'яків“ були розроблені для пошуку в мережі інших комп'ютерів з вільними ресурсами щоб забезпечувати можливість проведення розподілених обчислень. При правильному використанні технологія „черв'яків“ може бути надзвичайно корисною. Наприклад, „черв'як“ World Wide Web Worm формує індекс пошуку ділянок Web. Проте „черв'як“ легко перетворюється у шкідливу програму.

Мережні „черв'яки“ є найнебезпечнішим видом зловмисних програм, оскільки об'єктом їх нападу може стати будь-який з величезної кількості комп'ютерів, підключених до глобальної мережі Інтернет, чи інших мереж. Для захисту від „черв'яка“ застосовують засоби, направлені на блокування несанкціонованого доступу до внутрішньої мережі.

Слід зазначити, що „троянські коні“, комп'ютерні віруси та мережні „черв'яки“ відносяться до найнебезпечніших загроз ІС. Для захисту від зловмисних програм необхідно застосовувати ряд заходів [iii]:

- виключення несанкціонованого доступу до виконуваних файлів;
- тестування нових програм;
- контроль цілісності виконуваних файлів та системних областей;
- створення замкнутого середовища виконання програм.

1.3. Забезпечення безпеки інформаційних систем

Основним призначенням інформаційної системи є збір, зберігання, обробка та видача інформації, у зв'язку з чим проблема забезпечення інформаційної безпеки є для ІС центральною. Забезпечення безпеки ІС передбачає організацію протидії будь-якому несанкціонованому вторгненню в процес функціонування ІС, а також спробам модифікації, викрадення, виведення з ладу чи знищення її компонентів, – захист усіх компонентів ІС – апаратних засобів, програмного забезпечення, даних та персоналу. Існує два

підходи до проблеми забезпечення безпеки ІС: фрагментарний та комплексний [iii].

Фрагментарний підхід направлений на протидію чітко визначеним загрозам у заданих умовах. Прикладами такого підходу є окремі засоби управління доступом, автономні засоби шифрування, спеціалізовані антивірусні програми тощо. Перевагою такого підходу є висока вибірковість до конкретної загрози. Суттєвим недоліком такого підходу є відсутність єдиного захищеного середовища обробки інформації. Фрагментарні міри захисту інформації забезпечують захист конкретних об'єктів ІС тільки від конкретної загрози. Навіть невеликі видозміни загрози приводять до втрати ефективності захисту.

Комплексний підхід орієнтований на створення захищеного середовища обробки інформації в ІС, яке об'єднує в єдиний комплекс різноманітні заходи протидії загрозам. Організація захищеного середовища обробки інформації дозволяє гарантувати певний рівень безпеки ІС, що є неодмінною перевагою комплексного підходу. Основними недоліками цього підходу є: обмеження на свободу дій користувачів ІС, велика чутливість до помилок встановлення та настроювання засобів захисту, складність управління.

Комплексний підхід застосовують для захисту ІС великих організацій, та для невеликих ІС, що виконують відповідальні задачі чи обробляють особливо важливу інформацію. Порушення безпеки інформації в ІС великих організацій може принести великі збитки як самим організаціям, так і їх клієнтам. Тому такі організації вимушені надавати особливу увагу гарантіям безпеки та реалізовувати комплексний захист. Комплексного підходу притримуются більшість державних та крупних комерційних підприємств та закладів.

Комплексний підхід до проблеми забезпечення безпеки базується на розробленій для конкретної ІС політиці безпеки. ***Політика безпеки*** являє собою набір норм, правил та практичних рекомендацій, на яких базується управління, захист та розподіл інформації в ІС [ii]. Політика безпеки регламентує ефективну роботу засобів захисту ІС. Вона охоплює усі особливості процесу обробки інформації, визначаючи поведінку системи в різних ситуаціях. Політика безпеки реалізується засобами адміністративно-організаційних заходів, фізичних та програмно-технічних засобів та визначає архітектуру систем захисту. Для конкретної організації політика безпеки повинна носити індивідуальний характер і залежати від конкретної технології обробки інформації та використовуваних програмних і технічних засобів. Політика безпеки визначається способом управління доступом, який визначає порядок доступу до об'єктів системи. Розрізняють два основних види політики

безпеки: ***вибіркову*** та ***повноважну***.

Вибіркова політика безпеки базується на вибірковому способі управління доступом. ***Вибіркове управління доступом*** характеризується заданою адміністратором множиною дозволених відношень доступу (зазвичай у вигляді записів типу <об'єкт, суб'єкт, тип доступу>). Зазвичай для описання властивостей вибіркового управління доступом застосовують математичну модель на основі матриці доступу [iii]. ***Матриця доступу*** представляє собою матрицю, в якій стовпчик відповідає об'єкту системи, а рядок – суб'єкту. На перетині стовпця і рядка вказується тип дозволеного доступу суб'єкту до об'єкту. Зазвичай виділяють такі типи доступу до об'єкту, як „доступ для читання", „доступ для запису", „доступ для виконання" тощо. Матриця доступу є найпростішим підходом до моделювання систем управління доступом і часто є основою для складніших моделей, що адекватніше описують реальні ІС. Вибіркова політика безпеки широко застосовується в ІС комерційного сектору, оскільки її реалізація відповідає вимогам комерційних організацій з розмежування доступу та підзвітності і має прийнятну вартість.

Повноважна політика безпеки базується на повноважному (мандатному) способі управління доступом. ***Повноважне управління доступом*** характеризується сукупністю правил надання доступу, визначених на множині атрибутів безпеки суб'єктів та об'єктів, наприклад, залежно від мітки конфіденційності інформації та рівня допуску користувача. Повноважне управління доступом передбачає, що:

- усі суб'єкти і об'єкти системи однозначно ідентифіковані;
- кожному об'єкту системи присвоєна мітка конфіденційності інформації, що визначає цінність інформації, яка міститься в ньому;
- кожному суб'єкту системи присвоєно певний рівень допуску, який визначає максимальне значення мітки конфіденційності інформації об'єктів, до яких має доступ суб'єкт.

Чим важливішим є об'єкт, тим вище його мітка конфіденційності. Тому найбільш захищеними виявляються об'єкти з найвищим значенням мітки конфіденційності. Основним призначенням повноважної політики безпеки є регулювання доступу суб'єктів системи до об'єктів з різними рівнями конфіденційності, уникнення витікання інформації з верхніх рівнів посадової ієрархії на нижні, а також блокування можливих проникнень з нижніх рівнів на верхні.

Крім управління доступом суб'єктів до об'єктів системи, проблема захисту інформації має ще один аспект. Для отримання інформації про якийсь об'єкт системи зовсім не обов'язково шукати шляхи несанкціонованого

доступу до нього. Необхідну інформацію можна отримати, спостерігаючи за роботою з потрібним об'єктом – використовуючи канали витікання інформації. В системі завжди існують інформаційні потоки. Тому адміністратору потрібно визначити, які потоки інформації є „легальними" – не приводять до витікання інформації, а які – приводять. Тому виникає необхідність розробки правил, що регламентують управління інформаційними потоками в системі. Зазвичай управління інформаційними потоками застосовується в рамках вибіркової чи повноважної політики, доповнюючи їх і сприяючи підвищенню надійності системи захисту. Вибіркове і повноважне управління доступом та управління інформаційними потоками є тим фундаментом, на якому будується уся система захисту.

> Під ***системою захисту*** ІС розуміють сукупність правових та морально-етичних норм, адміністративно-організаційних заходів, фізичних та програмно-технічних засобів, направлених на протидію загрозам ІС з метою зведення до мінімуму можливості нанесення збитків.

Процес побудови системи захисту включає такі етапи [iii]:

- аналіз можливих загроз ІС;
- планування системи захисту;
- реалізація системи захисту;
- супровід системи захисту.

Етап аналізу можливих загроз ІС необхідний для фіксації стану ІС (конфігурації апаратних і програмних засобів, технології обробки інформації) та визначення можливих впливів на компоненти системи. Практично неможливо забезпечити захист інформаційної системи від усіх впливів, оскільки неможливо повністю встановити (визначити) усі загрози та способи їх реалізації. Тому з усієї множини ймовірних впливів вибирають тільки такі впливи, які можуть реально відбутися та нанести серйозні збитки.

На ***етапі планування*** формулюється система захисту, як єдина сукупність заходів протидії загрозам різної природи. За способами реалізації усі міри забезпечення безпеки комп'ютерних систем поділяються на [vii]:

- правові (законодавчі);
- морально-етичні;
- адміністративні;
- фізичні;
- апаратно-програмні.

Перелічені заходи безпеки ІС можна розглядати як послідовність бар'єрів чи кордонів захисту інформації. Для того, щоб отримати доступ до захищеної інформації, потрібно послідовно подолати кілька кордонів захисту. Розглянемо

їх детальніше.

Перший кордон захисту, що постає на шляху людини, яка робить спробу здійснити несанкціонований доступ до інформації, є суто правовим. Цей аспект захисту інформації пов'язаний з необхідністю дотримання юридичних норм при передачі і обробці інформації. До ***правових мір*** захисту інформації відносяться діючі в країні закони, укази та інші нормативні акти, які регламентують правила використання інформації обмеженого використання та відповідальність за їх порушення. Цим вони перешкоджають несанкціонованому використанню інформації та є стримуючим фактором для потенційних порушників.

Другий кордон захисту утворюють ***морально-етичні засоби***. Етичний момент у дотриманні вимог захисту має дуже велике значення. Надзвичайно важливо, щоб особи, які мають доступ до комп'ютерів, працювали в здоровому морально-етичному кліматі. До морально-етичних засобів протидії відносяться різноманітні норми поведінки, які традиційно склалися чи складаються в суспільстві у зв'язку з розповсюдженням комп'ютерів у країні. Ці норми в переважній більшості не є обов'язковими і законодавчо затвердженими, але їх недотримання зазвичай приводить до падіння престижу особи, групи осіб чи організації. Морально-етичні норми бувають як „неписаними" (наприклад, загальноприйняті норми чесності, патріотизму тощо), так і оформлені в деяке зведення правил чи приписів. Наприклад, „Кодекс професійної поведінки членів Асоціації користувачів ЕОМ США" [viii] розглядає як неетичні дії, які зумисно чи незумисно:

- порушують нормальне функціонування комп'ютерних систем;
- викликають невиправдані затрати ресурсів (машинного часу, пам'яті, каналів зв'язку тощо);
- порушують цілісність інформації;
- порушують інтереси інших законних користувачів тощо.

Третім кордоном, який перешкоджає неправочинному використанню інформації, є адміністративні заходи. Адміністратори усіх рангів з врахуванням усіх правових норм та соціальних аспектів визначають адміністративні заходи захисту інформації. ***Адміністративні заходи*** захисту відносяться до заходів організаційного характеру. Вони регламентують:

- процеси функціонування ІС;
- використання ресурсів ІС;
- діяльність персоналу;
- порядок взаємодії користувачів із системою для того, щоб якомога сильніше ускладнити чи виключити можливість реалізації загроз безпеці.

Адміністративні заходи включають [і]:

- розробку правил роботи з інформацією в ІС;
- сукупність дій при проектуванні та обладнанні обчислювальних центрів та інших об’єктів ІС (врахування впливу стихійних явищ, пожеж, охорона приміщень тощо);
- сукупність дій при підборі та підготовці персоналу (перевірка нових співробітників, ознайомлення їх з порядком роботи з конфіденційною інформацією, із ступенем відповідальності за порушення правил роботи з інформацією, створення умов, при яких персоналу було б невигідно допускати зловживання і т.д.);
- організацію надійного пропускного режиму;
- організацію обліку, зберігання, використання та знищення документів і носіїв з конфіденційною інформацією;
- розподіл реквізитів розмежування доступу (паролів, повноважень тощо);
- організацію прихованого контролю за роботою користувачів та персоналу ІС;
- сукупність дій при проектуванні, розробці, ремонті та модифікації обладнання і програмного забезпечення (сертифікація технічних та програмних засобів, строге санкціонування, розгляд та затвердження усіх змін, перевірка на відповідність нормам захисту, документальна фіксація змін тощо).

Слід зазначити, що поки не будуть реалізовані ефективні заходи адміністративного захисту ІС, інші заходи, без сумніву, будуть неефективними. Адміністративно-організаційні заходи можуть здатися не цікавими і рутинними порівняно з морально-етичними та неконкретними, порівняно з апаратно-програмними. Проте вони представляють собою потужний бар’єр на шляху незаконного використання інформації та надійну базу для інших рівнів захисту.

Четвертим кордоном є ***фізичні засоби захисту***. До фізичних засобів захисту відносяться різноманітні механічні, електро- та електронно-механічні пристрої чи споруди, які спеціально призначені для створення фізичних перешкод на можливих шляхах проникнення та доступу потенційних порушників до компонентів системи та захищеної інформації.

П’ятим кордоном є ***апаратно-програмні засоби захисту***. До них відносяться різноманітні електронні пристрої та спеціальні програми, які реалізують самостійно чи в комплексі з іншими засобами наступні способи захисту:

- ідентифікацію (розпізнавання) та автентифікацію (перевірка справжності) суб’єктів (користувачів, процесів) ІС;
- розмежування доступу до ресурсів ІС;
- контроль цілісності даних;

- забезпечення конфіденційності даних;
- реєстрацію та аналіз подій, що відбуваються в ІС;
- резервування ресурсів та компонентів ІС.

Більшість з перелічених методів захисту реалізуються криптографічними методами захисту інформації.

При проектуванні ефективної системи захисту слід враховувати ряд принципів, що відображають основні положення з безпеки інформації. До числа цих принципів відносяться наступні [iii]:

- ***Економічна ефективність***. Вартість засобів захисту повинна бути меншою, ніж розміри можливих збитків.
- ***Мінімум привілеїв***. Кожний користувач повинен мати мінімальний набір привілеїв, необхідних для роботи.
- ***Простота***. Захист тим ефективніший, чим легше користувачу з ним працювати.
- ***Можливість примусового відключення захисту***. За нормального функціонування захист не повинен відключатися. Тільки в особливих випадках співробітник зі спеціальними повноваженнями може відключити систему захисту.
- ***Відкритість проектування та функціонування механізмів захисту***. Фахівці, що мають відношення до системи захисту, повинні повністю уявляти собі принципи її функціонування і у випадку виникнення ускладнень, адекватно на них реагувати.
- ***Загальний контроль***. Будь-які винятки з множини контрольованих суб'єктів та об'єктів захисту знижують захищеність автоматизованого комплексу обробки інформації.
- ***Незалежність системи захисту від суб'єктів захисту***. Особи, що займаються розробкою системи захисту, не повинні бути в числі тих, кого ця система контролюватиме.
- ***Звітність та підконтрольність***. Система захисту повинна надавати докази коректності своєї роботи.
- ***Відповідальність***. Передбачається особиста відповідальність осіб, що забезпечують безпеку інформації.
- ***Ізоляція та розподіл***. Об'єкти захисту доцільно розділяти на групи таким чином, щоб порушення захисту в одній із груп не впливало на безпеку інших груп.
- ***Повнота та узгодженість***. Надійна система захисту повинна бути повністю сертифікована, протестована та узгоджена.
- ***Параметризація***. Захист стає ефективнішим та гнучкішим, якщо він допускає зміну своїх параметрів зі сторони адміністратора.
- ***Принцип ворожого оточення***. Система захисту повинна проектуватися з розрахунку на вороже оточення. Розробники повинні припускати, що користувачі мають найгірші наміри, що вони будуть робити серйозні помилки та шукати шляхи обходу механізмів захисту.

- ***Залучення людини***. Найважливіші та критичні рішення повинні прийматися людиною.
- ***Відсутність надлишкової інформації про існування механізмів захисту***. Існування механізмів захисту повинно бути, наскільки це можливо, приховане від користувачів, робота яких повинна контролюватися.

Результатом ***етапу планування*** є розгорнутий план захисту ІС, який містить перелік захищуваних компонентів ІС та можливих впливів на них, мету захисту інформації, правила обробки інформації, що забезпечують її захист від різноманітних впливів, а також опис запланованої системи захисту інформації.

Суть ***етапу реалізації*** системи захисту полягає у встановленні та настроюванні засобів захисту, необхідних для реалізації запланованих правил обробки інформації.

Заключний ***етап супроводу*** полягає у контролі роботи системи, реєстрації подій, що відбуваються в ній, та їх аналізі з метою виявлення порушень безпеки, корекції системи захисту.

1.4. Принципи криптографічного захисту інформації

> ***Криптографія*** представляє собою сукупність методів перетворення даних, направлених на те, щоб зробити ці дані незрозумілими для усіх крім респондента, якому адресуються дані.

Такі перетворення дозволяють розв’язати дві головні проблеми захисту даних [іх]: ***проблему конфіденційності*** (шляхом усунення можливості отримання корисної інформації з каналу зв’язку) та ***проблему цілісності*** (шляхом усунення можливості змінювати повідомлення противником). Проблеми конфіденційності та цілісності інформації тісно зв’язані між собою, у зв’язку з чим методи розв’язання однієї з них часто можна застосовувати для розв’язання іншої.

Узагальнена схема криптографічної системи, що забезпечує шифрування інформації при її передачі по каналах зв’язку, наведена на рис. 1.

Відправник генерує ***відкритий текст*** вихідного повідомлення M, яке повинно бути передане законному ***отримувачу*** по незахищеному каналу. За каналом слідкує ***перехоплювач*** з метою перехопити та розкрити повідомлення. Для того, щоб перехоплювач не зміг розкрити зміст повідомлення M, відправник його шифрує за допомогою оборотного перетворення E_K та отримує ***шифротекст*** (чи ***криптограму***) $C=E_K(M)$, який відправляє отримувачу.

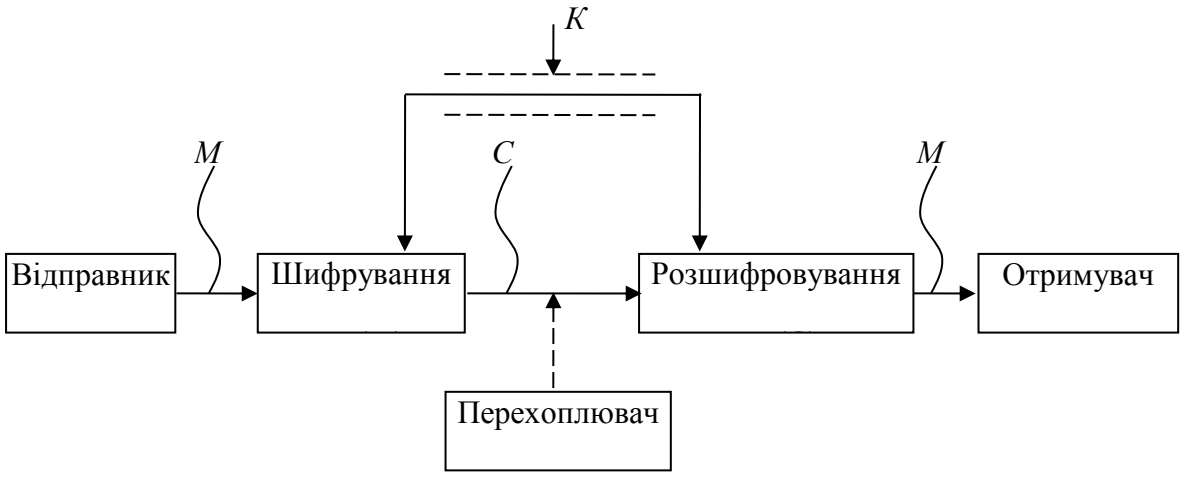

Рис. 1. Узагальнена схема криптосистеми

Законний отримувач, прийнявши шифротекст *C*, розшифровує його за допомогою оберненого перетворення $D=E_K^{-1}$ та отримує вихідне повідомлення у вигляді відкритого тексту *M*:

$$D_K(C)=E_K^{-1}(E_K(M))=M.$$

Перетворення E_K вибирається із сімейства криптографічних перетворень, які називаються ***криптоалгоритмами***. Параметр, за допомогою якого вибирається окреме використовуване перетворення, називається ***криптографічним ключем*** *K*. Краптосистеми мають різні варіанти реалізації: набір інструкцій, апаратні засоби, комплекс комп'ютерних програм, які дозволяють зашифрувати відкритий текст та розшифрувати шифротекст різними способами, один з яких вибирається за допомогою конкретного ключа *K*. Висловлюючись більш формально, криптографічна система – це одно параметричне сімейство $(E_K)_{K\in\overline{K}}$ оборотних перетворень

$$E_K : \overline{M} \to \overline{C}$$

з простору $\overline{M}$ повідомлень відкритого тексту в простір $\overline{C}$ шифрованих текстів [ix]. Параметр *K* (ключ) вибирається з кінцевої множини $\overline{K}$, яка називається ***простором ключів***.

Взагалі кажучи, перетворення шифрування може бути симетричним чи асиметричним по відношенню до перетворення розшифровування. Ця важлива властивість функції перетворення визначає два класи криптосистем [x]:

- ***симетричні*** (одноключові) криптосистеми;
- ***асиметричні*** (двохключові) криптосистеми (з відкритим ключем).

Схема симетричної криптосистеми з одним секретним ключем була представлена на рис. 1. В ній використовуються однакові секретні ключі в блоках шифрування та розшифровування. Узагальнена схема асиметричної криптосистеми з двома різними ключами K_1 та K_2 представлена на рис. 2. В цій криптосистемі один із ключів є відкритим, а другий – секретним.

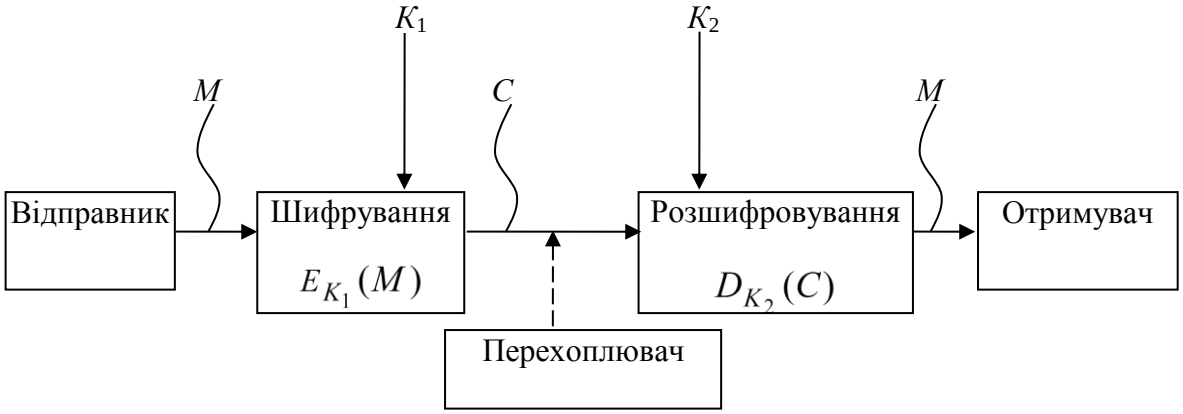

Рис. 2. Узагальнена схема асиметричної криптографії з відкритим ключем

У симетричній криптосистемі секретний ключ потрібно передавати відправнику та отримувачу по захищеному каналу розповсюдження ключів, наприклад такому, як кур'єрська служба. На рис. 1 цей канал показано „екранованою" лінією. В асиметричній криптосистемі передають по незахищеному каналу тільки відкритий ключ, а секретний ключ зберігають на місці його генерації.

На рис. 3 показано потік інформації у криптосистемі у випадку активних дій перехоплювача. Активний перехоплювач не тільки зчитує усі шифротексти, що передаються по каналу, а також може спробувати змінити їх на свій розсуд.

Будь-яка спроба зі сторони перехоплювача розшифрувати шифротекст C для отримання відкритого тексту M чи зашифрувати свій власний текст M' для отримання правдоподібного шифротексту C', не маючи справжнього ключа, називається ***криптоаналітичною атакою***. Якщо спроби криптоаналітичних атак не досягають поставленої мети і криптоаналітик не може, не маючи справжнього ключа, вивести M із C чи C' із M', то вважають, що така криптосистема є ***крипостійкою.***

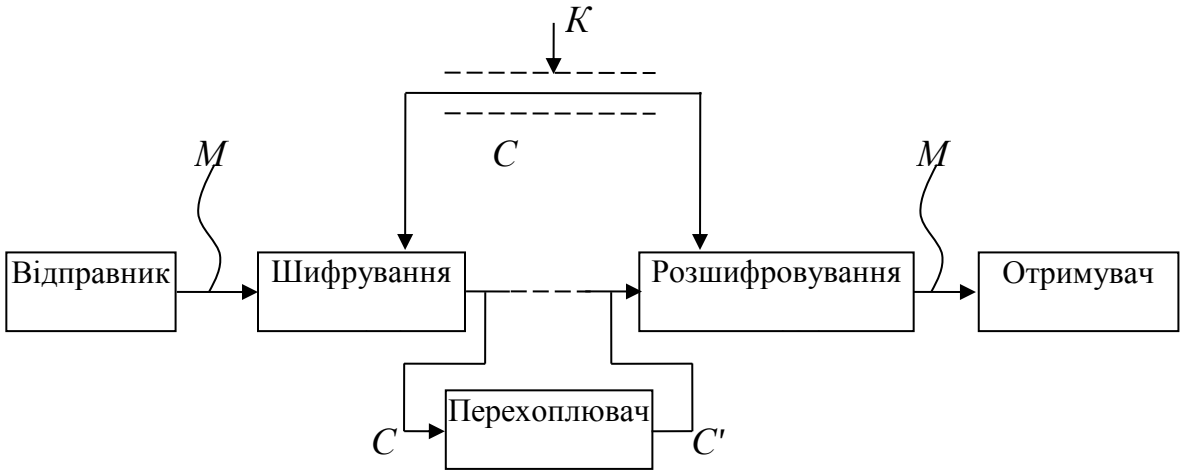

Рис. 3. Потік інформації в криптосистемі при активному перехопленні повідомлень

Криптоаналіз – це наука про розкриття вихідного тексту зашифрованого повідомлення без доступу до ключа.

Успішний аналіз може розкрити вихідний текст чи ключ. Він дозволяє також виявляти слабкі місця в криптосистемі, що, в підсумку, приводить до тих же результатів.

Фундаментальне правило криптоаналізу, вперше сформульоване голландцем А. Керкхоффом ще в XIX столітті, полягає в тому, що стійкість шифру (криптосистеми) повинна визначатися тільки секретністю ключа [x]. Іншими словами, правило Керкхоффа полягає в тому, що весь алгоритм шифрування, крім знання секретного ключа, відомий криптоаналітику противника. Останнє зумовлене тим, що криптосистема, яка реалізує сімейство криптографічних перетворень, зазвичай розглядається як відкрита система. Такий важливий принцип відображає надзвичайно важливий принцип технології захисту інформації: захищеність системи не повинна залежати від секретності чогось такого, що неможливо швидко змінити у випадку витоку секретної інформації. Зазвичай криптосистема являє собою сукупність апаратних та програмних засобів, які можна змінити тільки при значних затратах часу та коштів, тоді як ключ є об’єктом, який легко змінити. Саме тому стійкість криптосистеми визначаєься тільки секретністю ключа. Друге, майже загальноприйняте припущення в криптоаналізі полягає в тому, що криптоаналітик має в своєму розпорядженні шифротексти повідомлень.

Розрізняють шість основних типів криптоаналітичних атак [ix]. Усі вони формулюються вважаючи, шо криптоаналітику відомий алгоритм шифрування

та шифротексти повідомлень.

Криптоаналітична атака за наявності тільки відомого шифротексту. Криптоаналітик має тільки шифротексти C_1, C_2, … C_i кількох повідомлень, причому усі вони зашифровані з використанням одного і того ж алгоритму шифрування E_K. Робота криптоаналітика полягає у тому, щоб розкрити вихідні тексти M_1, M_2, … M_i якомога більшої кількості повідомлень чи, ще краще, вирахувати ключ K, використаний для шифрування цих повідомлень з тим, щоб розшифрувати й інші повідомлення, зашифровані цим ключем.

Криптоаналітична атака при наявності відомого відкритого тексту. Криптоаналітик має доступ не тільки до шифротекстів C_1, C_2, … C_i кількох повідомлень, а й до відкритих текстів M_1, M_2, … M_i цих повідомлень. Його робота полягає у знаходженні ключа K, що використовується при шифруванні цих повідомлень, чи алгоритму розшифровування D_K будь-яких нових повідомлень, зашифрованих тим же самим ключем.

Криптоаналітична атака при можливості вибору відкритого тексту. Криптоаналітик не тільки має доступ до шифротекстів C_1, C_2, … C_i та зв'язаних з ними відкритих текстів M_1, M_2, … M_i кількох повідомлень, а й може за бажанням вибрати відкриті тексти, які потім отримує у зашифрованому вигляді. Такий криптоаналіз є ефективнішим, порівняно з відомим відкритим текстом, тому, що криптоаналітик може вибрати для шифрування такі блоки відкритого тексту, які дадуть більше інформації про ключ. Робота криптоаналітика полягає у пошуку ключа K, використаного для шифрування повідомлень, чи алгоритму розшифровування D_K нових повідомлень, зашифрованих тим же ключем.

Криптоаналітична атака з адаптивним вибором відкритого тексту. Це особливий варіант атаки з вибором відкритого тексту. Криптоаналітик може не тільки вибирати відкритий текст, який потім зашифровується, а й змінювати свій вибір залежно від результатів попереднього шифрування. При криптоаналізі з простим вибором відкритого тексту криптоаналітик зазвичай може вибрати кілька крупних блоків відкритого тексту для їх шифрування, тоді як при криптоаналізі з адаптивним вибором відкритого тексту він має можливість спочатку вибрати менший пробний блок відкритого тексту, потім вибрати наступний блок на основі першого вибору і т.д. Така атака надає криптоаналітику ще більше можливостей, порівняно з першими трьома типами.

Криптоаналітична атака з використанням вибраного шифротексту.

Криптоаналітик може вибрати для розшифровування різні шифротексти C_1, C_2, … C_i та має доступ до розшифрованих відкритих текстів M_1, M_2, … M_i. Наприклад, криптоаналітик отримав доступ до захищеного від несанкціонованого доступу блоку, який виконує автоматичне розшифровування. Завдання криптоаналітика полягає в знаходженні ключа. Цей тип криптоаналізу представляє особливий інтерес для розкриття алгоритмів з відкритим ключем.

Криптоаналітична атака методом повного перебору усіх можливих ключів. Ця атака передбачає використання криптоаналітиком відомого шифротексту та здійснюється шляхом повного перебору усіх можливих ключів з перевіркою, чи є осмисленим відкритий текст. Такий підхід вимагає залучення надзвичайно потужних обчислювальних ресурсів і іноді називається ***силовою атакою***.

Існують і інші, менш розповсюджені криптоаналітичні атаки.

1.5. Апаратно-програмні засоби захисту комп'ютерної інформації

Перші операційні системи для персональних комп'ютерів не мали власних засобів захисту, що і породило проблему створення додаткових засобів захисту. Актуальність цієї проблеми практично не зменшилася з появою більш потужних ОС з розвинутими підсистемами захисту. Це обумовлено тим, що більшість систем не здатні захистити дані, які перебувають за її межами, наприклад при використанні мережного інформаційного обміну. Апаратно-програмні засоби, що забезпечують підвищений рівень захисту, можна розбити на п'ять основних груп, рис. 4 [iv].

Першу групу утворюють ***системи ідентифікації та автентифікації користувачів***. Такі системи застосовуються для обмеження доступу випадкових та незаконних користувачів до ресурсів комп'ютерної системи. Загальний алгоритм роботи цих систем полягає в тому, щоб отримати від користувача інформацію, яка посвідчує його особу, перевірити її справжність і потім надати (чи не надати) цьому користувачу можливість роботи з системою. При побудові подібних систем виникає проблема вибору інформації, на основі якої здійснюються процедури ідентифікації та автентифікації користувача. Можна виділити наступні типи:

1) секретна інформація, якою володіє користувач (пароль, персональний ідентифікатор, секретний ключ тощо); цю інформацію користувач повинен запам'ятати або ж можуть бути застосовані спеціальні засоби зберігання такої інформації;
2) фізіологічні параметри людини (відбитки пальців, рисунок райдужної

оболонки ока) чи особливості поведінки людини (особливості роботи на клавіатурі – „клавіатурний почерк“ тощо).

Системи ідентифікації, що базуються на першому типі інформації, прийнято вважати ***традиційними***. Системи ідентифікації, що використовують другий тип інформації, називають ***біометричними***. Слід відзначити тенденцію все більшого використання біометричних систем ідентифікації.

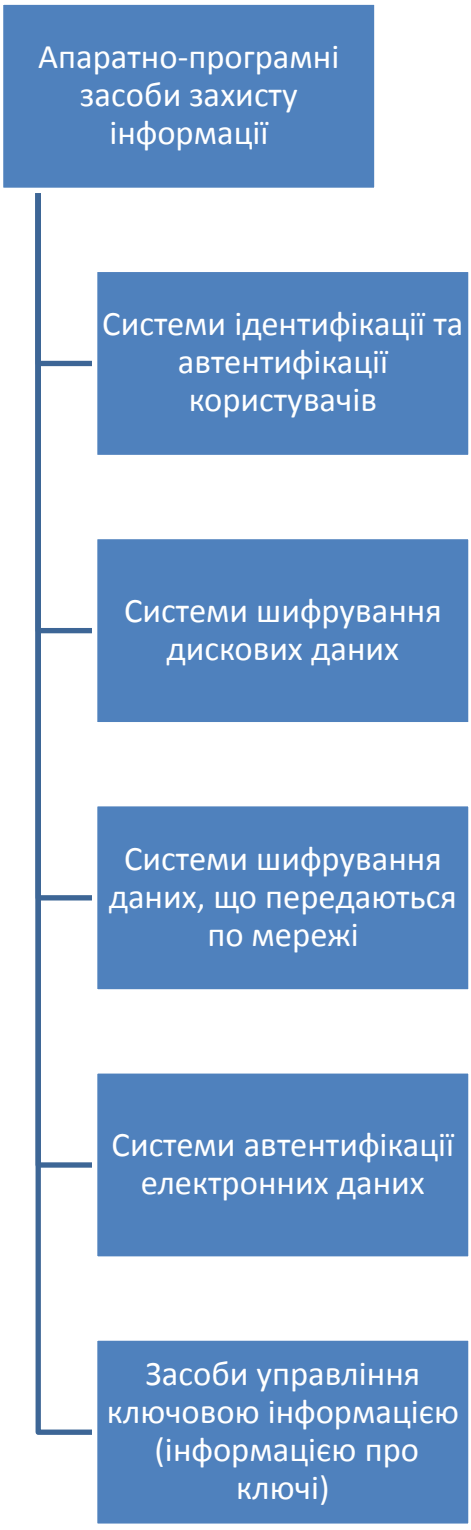

Рис. 4. Апаратно-програмні засоби захисту комп’ютерної інформації

Другу групу засобів, що забезпечують підвищений рівень захисту, складають системи ***шифрування дискових даних***. Основна задача, що вирішується такими системами, полягає у захисті від несанкціонованого використання даних, розміщених на магнітних носіях інформації. Забезпечення конфіденційності даних, що розміщуються на магнітних носіях, здійснюється шляхом їх шифрування з використанням симетричних алгоритмів шифрування. Основною класифікаційною ознакою для комплексів шифрування служить їх рівень вбудованості у комп'ютерну систему.

Робота прикладних програм з дисковими накопичувачами складається з двох етапів – ***логічного*** та ***фізичного***.

Логічний етап відповідає рівню взаємодії прикладної програми з операційною системою (наприклад, виклик сервісних функцій читання/запису даних). На цьому рівні основним об'єктом є файл.

Фізичний етап відповідає рівню взаємодії операційної системи та апаратури. У якості об'єктів цього рівня виступають структури фізичної організації даних – сектори диску.

В результаті системи шифрування даних можуть здійснювати криптографічні перетворення даних на рівні файлів (захищаються окремі файли) та на рівні дисків (захищаються цілі диски).

Іншою класифікаційною ознакою систем шифрування дискових даних є спосіб їх функціонування. За способом функціонування системи шифрування дискових даних поділяються на два класи:

1) системи ***прозорого*** шифрування;
2) системи, які спеціально викликаються для здійснення шифрування.

У системах ***прозорого шифрування*** (шифрування „на льоту“) криптографічні перетворення здійснюються в режимі реального часу непомітно для користувача. Наприклад, користувач записує підготовлений у текстовому редакторі документ на захищуваний диск, а система в процесі запису здійснює його шифрування. Системи другого класу зазвичай представляють собою утиліти, які необхідно спеціально викликати для виконання шифрування. До них відносяться, наприклад, архіватори з вбудованими засобами парольного захисту.

До третьої групи засобів, що забезпечують підвищений рівень захисту, відносяться ***системи шифрування даних, що передаються по комп'ютерним мережам***. Розрізняють два основних способи шифрування: ***канальне***

шифрування та ***кінцеве*** (абонентське, термінальне) шифрування.

У випадку ***канального шифрування*** захищається уся інформація, що передається по каналу зв'язку, включаючи і службову. Відповідні процедури шифрування реалізуються, наприклад, за допомогою протоколу канального рівня семирівневої еталонної моделі взаємодії відкритих систем OSI [**Ошибка! Закладка не определена.**]. Цей спосіб має суттєву перевагу – вбудовування процедур шифрування у канальний рівень дозволяє використовувати апаратні засоби, що сприяє підвищенню продуктивності системи. Однак у даного підходу є й суттєві недоліки:

- шифруванню на даному рівні підлягає уся інформація, включаючи службові дані транспортних протоколів, що ускладнює механізм маршрутизації мережних пакетів та вимагає розшифровування даних в пристроях проміжної комутації (шлюзах, ретрансляторах тощо);
- шифрування службової інформації, неминуче на даному рівні, може привести до появи статистичних закономірностей у шифруванні даних, що впливає на надійність захисту і накладає обмеження на використання криптографічних алгоритмів.

Кінцеве (***абонентське***) ***шифрування*** дозволяє забезпечити конфіденційність даних, що передаються між двома прикладними об'єктами (абонентами). Кінцеве шифрування реалізується за допомогою протоколу прикладного чи представницького рівня еталонної моделі OSI [**Ошибка! Закладка не определена.**]. В цьому випадку захищається тільки зміст повідомлення, вся ж службова інформація залишається відкритою. Даний спосіб дозволяє уникнути проблем, пов'язаних із шифруванням службової інформації, але при цьому виникають інші проблеми. Зокрема, зловмисник, який має доступ до каналів зв'язку комп'ютерної мережі, отримує можливість аналізувати інформацію про структуру обміну повідомленнями, наприклад, про відправника і отримувача, про час і умови передачі даних, а також про об'єм даних, що передаються.

Четверту групу засобів захисту складають ***системи автентифікації електронних даних***. При обміні електронними даними по мережах зв'язку виникає проблема автентифікації автора документу та самого документу – встановлення справжності автора та перевірка відсутності змін в отриманому документі. Для автентифікації електронних даних застосовують ***код автентифікації повідомлення*** (***імітовставку***) чи ***електронний цифровий підпис***. При формуванні коду автентифікації повідомлення та електронного цифрового підпису використовують різні типи систем шифрування.

Код автентифікації повідомлення формують за допомогою

симетричних систем шифрування даних. Зокрема, симетричний алгоритм шифрування даних DES при роботі в режимі зчеплення блоків шифру CBC дозволяє сформувати за допомогою секретного ключа та початкового вектора IV код автентифікації повідомлення MAC (Message Authentication Code) [**Ошибка! Закладка не определена.**]. Перевірка цілісності прийнятого повідомлення здійснюється шляхом перевірки коду MAC отримувачем повідомлення. Аналогічні можливості надає алгоритм ГОСТ 28147-89 [**Ошибка! Закладка не определена.**], в якому передбачено режим вироблення імітовставки, яка забезпечує ***імітозахист*** – захист системи шифрування зв'язку від нав'язування неправдивих даних. ***Імітовставка*** виробляється з відкритих даних шляхом спеціального перетворення шифрування з використанням секретного ключа і передається по каналу зв'язку в кінці зашифрованих даних. Імітовставка перевіряється отримувачем повідомлення, який володіє секретним ключем, шляхом повторення процедури, виконаної раніше відправником, над отриманими відкритими даними.

Електронний цифровий підпис (ЕЦП) представляє собою відносно невеликий об'єм додаткової автентифікуючої цифрової інформації, що передається разом із „підписаними" даними. Для реалізації ЕЦП використовуються принципи асиметричного шифрування. Система ЕЦП включає процедуру формування цифрового підпису відправником з використанням секретного ключа відправника та процедуру перевірки підпису отримувачем з використанням відкритого ключа відправника.

П'яту групу засобів, що забезпечують підвищений рівень захисту, утворюють ***засоби управління ключовою інформацією***. Під ключовою інформацією тут розуміється сукупність усіх використовуваних в комп'ютерній системі чи мережі криптографічних ключів. Безпека будь-якого криптографічного алгоритму визначається використовуваними криптографічними ключами. У випадку ненадійного управління ключами зловмисник може заволодіти ключовою інформацією та отримати повний доступ до всієї інформації в комп'ютерній системі чи мережі. Основною класифікаційною ознакою засобів управління ключовою інформацією є вид функції управління ключами. Розрізняють такі основні види функцій управління ключами [ix]: генерація ключів, зберігання ключів та розповсюдження ключів.

Способи ***генерації ключів*** розрізняються для симетричних і асиметричних криптосистем. Для генерації ключів симетричних криптосистем використовуються апаратні та програмні засоби генерації випадкових чисел,

зокрема системи із застосуванням блочного симетричного алгоритму шифрування. Генерація ключів для асиметричних криптосистем є значно складнішою задачею у зв'язку з необхідністю отримання ключів з певними математичними властивостями.

Функція ***зберігання ключів*** передбачає організацію безпечного зберігання, обліку та знищення ключів. Для забезпечення безпечного зберігання та передачі ключів застосовують їх шифрування з використанням інших ключів. Такий підхід приводить до ***концепції ієрархії ключів***. До ієрархії ключів зазвичай входять головний ключ (майстер-ключ), ключ шифрування ключів та ключ шифрування даних. Слід зазначити, що генерація та зберігання майстер-ключів є критичними питаннями криптографічного захисту.

Розповсюдження ключів є найвідповідальнішим процесом в управлінні ключами. Цей процес повинен гарантувати секретність розповсюджуваних ключів, а також оперативність і точність їх розповсюдження. Розрізняють два основних способи розповсюдження ключів між користувачами комп'ютерної мережі:

- використання одного чи кількох центрів розповсюдження ключів;
- прямий обмін сеансовими ключами між користувачами.

2. Правовий захист інформації

Серед різних методів захисту інформації особлива роль відводиться правовому захисту інформації. При всіх своїх можливостях та обов'язковості використання, фізичні та програмно-технічні методи захисту не зможуть забезпечити безпеку інформаційних систем, якщо відсутня адекватна правова база, що регламентує діяльність в інформаційній сфері.

2.1. Комп'ютерні злочини

Розвиток обчислювальної техніки та її широке використання державними органами і приватними особами привели до виникнення та розповсюдження так званих комп'ютерних злочинів. Термін „комп'ютерна злочинність" було введено ще в 1960-х роках [xi]. Однак і досі продовжується дискусія про те, які протизаконні дії сюди відносяться. Було запропоновано ряд кримінально-правових визначень комп'ютерної злочинності. Часто це поняття трактується як злочин, який прямо чи опосередковано зв'язаний з ЕОМ, та включає у себе цілу серію незаконних актів, які здійснюються або за допомогою систем електронної обробки даних або проти таких систем. Інші джерела до комп'ютерної злочинності відносять будь-які дії, що тягнуть за собою незаконне втручання в майнові права, що виникають у зв'язку з використанням ЕОМ.

Виділяють наступні форми прояву комп'ютерної злочинності [xii]:

маніпуляції з ЕОМ, викрадення машинного часу, економічне шпигунство, саботаж, комп'ютерне здирництво, діяльність „хакерів".

Під комп'ютерними маніпуляціями розуміється неправомірна зміна вмісту носіїв інформації та програм, а також недопустиме втручання у процес обробки даних. Основні сфери комп'ютерних маніпуляцій наступні: здійснення покупок та кредитування (маніпуляції з розрахунками та платежами, доставка товару за фальшивою адресою); маніпуляції з товарами та рахунками дебеторів (знищення рахунків чи умов, оговорених у них, махінації з активами); розрахунки заробітної плати (зміна окремих статей нарахування платежів, внесення фіктивних осіб до платіжних відомостей). Поряд із безпосереднім незаконним використанням інформаційних систем, до категорії злочинів також відносяться дії, зв'язані із несанкціонованим доступом до мережі передачі інформації

Комп'ютерне шпигунство переслідує, як правило, економічні цілі. Злочини цієї категорії найчастіше здійснюються для отримання програм обробки даних, результатів наукових досліджень, конструкторської документації, відомостей про маркетингову стратегію конкурентів, адміністративних даних, відомостей про плани і технології виробництва тощо. Однією з найрозповсюдженішою на даний час формою комп'ютерних злочинів є діяльність „хакерів" – кваліфікованих програмістів та фахівців в інформаційних технологіях, які незаконно проникають в інформаційні мережі. Комп'ютерні злочини відрізняються від звичайних особливими просторово-часовими характеристиками. Такі дії здійснюються на протязі кількох секунд, а просторових обмежень для них взагалі не існує.

Як свідчить практика, одним з найважливіших способів підвищення ефективності боротьби з комп'ютерною злочинністю є створення належної правової основи для переслідування в кримінальному порядку осіб, винних у таких злочинах. На даний час розвиток правової основи для боротьби зі злочинами, об'єктом яких є „інтелектуальний" елемент ЕОМ, рухається в таких напрямках:

1. Створення кримінально-правових норм, які передбачають роздільний захист програмного забезпечення та баз даних, а також апаратних елементів електронно-обчислювальних систем;
2. Використання існуючого законодавства.

Незважаючи на те, що існуючі кримінальні закони є достатньо гнучкими для кваліфікації порушень цього типу, соціальні і технічні зміни створюють все нові й нові проблеми, частина з яких виходить за рамки будь-якої із сучасних правових систем. У зв'язку з цим підготовка нормативно-правових актів про комп'ютерну безпеку є надзвичайно складною, адже вона пов'язана з технологією, що постійно випереджає нормотворчий процес. Розвиток законодавства не завжди встигає за розвитком техніки та злочинним використанням її останніх досягнень

В комп'ютерних злочинах ЕОМ може бути як об'єктом, так і суб'єктом злочину. У тих випадках, коли ЕОМ є об'єктом злочину (їй завдається шкода шляхом фізичного пошкодження) не виникає проблем із застосуванням

існуючого законодавства. Але ті випадки, коли ЕОМ виступає в якості суб'єкту злочину являють собою нові правові ситуації. Існує ряд характерних рис злочинів, пов'язаних із використанням ЕОМ, які ускладнюють розслідування та висунення звинувачення по них. Крім юридичних проблем виникають і інші проблеми, з якими може зіткнутися слідство. Найважливішими з них є:

- складність виявлення злочинів, зв'язаних із використанням ЕОМ;
- велика дальність дії сучасних телекомунікаційних засобів дозволяє здійснювати незаконні маніпуляції з програмами та даними ЕОМ віддалено, практично з будь-якої точки світу;
- ускладнення в розумінні порядку роботи ЕОМ у технологічно складних випадках;
- інформація злочинного характеру, яка зберігається в пам'яті ЕОМ та служить доказом для звинувачення може бути ліквідована практично миттєво;
- звичайні методи фінансової ревізії у випадку таких злочинів неприйнятні, оскільки для передачі інформації використовуються електричні імпульси, а не фінансові документи.

Виникнення комп'ютерної злочинності та масштаби збитків викликали необхідність розробки законодавчих норм, що встановлюють відповідальність за подібні дії.

Особливості розслідування комп'ютерних злочинів. На перший погляд здається, що комп'ютерні злочини можуть бути розслідувані з використанням традиційного законодавства, що відноситься до крадіжки, розтрати, нанесення шкоди власності тощо. Проте невідповідність традиційного кримінального законодавства у застосуванні до цієї нової форми злочинів стає очевидним, оскільки потрібно встановити наявність усіх елементів складу традиційного злочину, здійсненого за допомогою ЕОМ. Наприклад, якщо зловмисник проник у приміщення, в якому розміщено ЕОМ, незаконно чи зі злочинною метою, тоді закон може бути застосований традиційно. Якщо злочинець проник у приміщення, в якому розміщено ЕОМ, для того, щоб завдати шкоди матеріальній частині комп'ютера, викрасти програму, то тільки вторгнення з незаконними намірами буде достатнім для висунення звинувачення по справі.

Однак, якщо особа робить спробу отримати доступ до даних в пам'яті ЕОМ для крадіжки цінної інформації чи з іншою метою, висунення звинувачення відповідно до традиційного закону навряд чи буде можливим, адже такий доступ зазвичай здійснюється з використанням віддаленого доступу. Також не завжди можна довести, як того вимагає закон, що мало місце якесь вилучення власності. Наприклад, комп'ютерна інформація чи дані можуть бути зчитані з віддаленого комп'ютера не зачіпаючи цілісність елементів матеріальної реалізації інформаційної системи тим самим відсутнє поняття вилучення власності.

2.2. Організаційно-правове забезпечення інформаційної безпеки

Простота та велика кількість способів доступу та модифікації інформації,

велика кількість кваліфікованих фахівців, широке використання у громадському виробництві спеціальних технічних засобів дозволяють зловмиснику практично в будь-який момент та в будь-якому місці здійснювати дії, що представляють загрозу інформаційній безпеці як в локальному, так і в глобальному масштабах.

Державна політика у сфері формування інформаційних ресурсів та інформатизації повинна бути направлена на створення умов для ефективного та якісного інформаційного забезпечення розв'язання стратегічних та оперативних задач соціального і економічного розвитку країни. Державні і недержавні організації, а також громадяни мають рівні права на розробку і виробництво інформаційних систем, технологій та засобів їх забезпечення.

Розвиток комп'ютерної техніки та її широке використання державними органами і приватними закладами привів до виникнення і широкого розповсюдження так званих комп'ютерних злочинів. Невідповідність традиційного кримінального законодавства у застосуванні до цієї форми злочинів стає очевидною, як тільки робиться спроба встановити наявність усіх елементів складу традиційного злочину, здійсненого за допомогою ЕОМ.

Як показують численні дослідження [xiii], найчастіше загроза інформаційним системам виходить від самих співробітників підприємства, хоча великої шкоди також завдають „хакери" та промисловий шпіонаж. У зв'язку з цим, як рекомендують фахівці з безпеки, особливу увагу слід звертати на нових співробітників – фахівців у галузі комп'ютерної техніки, програмування та захисту комп'ютерної інформації.

Організаційно-правове забезпечення інформаційної безпеки являє собою сукупність рішень, законів, нормативів, що регламентують як загальну організацію робіт із забезпечення інформаційної безпеки, так і створення та функціонування систем захисту інформації на конкретних об'єктах. Організаційно правова база має такі основні функції [ii]:

1. Розробка основних принципів віднесення відомостей, що мають конфіденційний характер, до захищуваної інформації.
2. Визначення системи органів та посадових осіб, що відповідають за забезпечення інформаційної безпеки в країні та порядку регулювання діяльності підприємств і організацій в цій області.
3. Створення повного комплексу нормативно-правових матеріалів, що регламентують питання забезпечення інформаційної безпеки як у країні в цілому, так і на конкретному об'єкті.
4. Визначення міри відповідальності за порушення правил захисту.
5. Визначення порядку вирішення спірних і конфліктних ситуацій з питань захисту інформації.

Під юридичними аспектами організаційно-правового забезпечення захисту інформації розуміється сукупність законів та інших нормативно-правових актів, за допомогою яких мали б досягатися наступні цілі [ii]:

- усі правила захисту інформації є обов'язковими для дотримання усіма особами, що мають відношення до конфіденційної інформації;
- узаконюються усі міри відповідальності за порушення правил захисту інформації;
- узаконюються (набувають юридичної сили) техніко-математичні рішення питань організаційно-правового забезпечення захисту інформації;
- узаконюються процесуальні процедури розв'язування ситуацій, що виникають у процесі функціонування системи захисту.

На рис. 19-21 представлено варіанти концептуальних моделей безпеки продукції, особистості та інформації. Навіть поверхневий аналіз цих моделей дає представлення про багатогранність дій та заходів із забезпечення інформаційної безпеки.

Розробка законодавчої бази інформаційної безпеки будь-якої держави є необхідною мірою, що задовольняє першочергову потребу в захисті інформації при розвитку соціально-економічних, політичних, військових напрямків розвитку цієї держави. Особлива увага з боку розвинутих країн до формування такої бази викликана все зростаючими затратами на боротьбу з „інформаційними" злочинами. Все це заставляє серйозно займатися питаннями законодавства із захисту інформації.

Рис. 19. Концептуальна модель безпеки особи

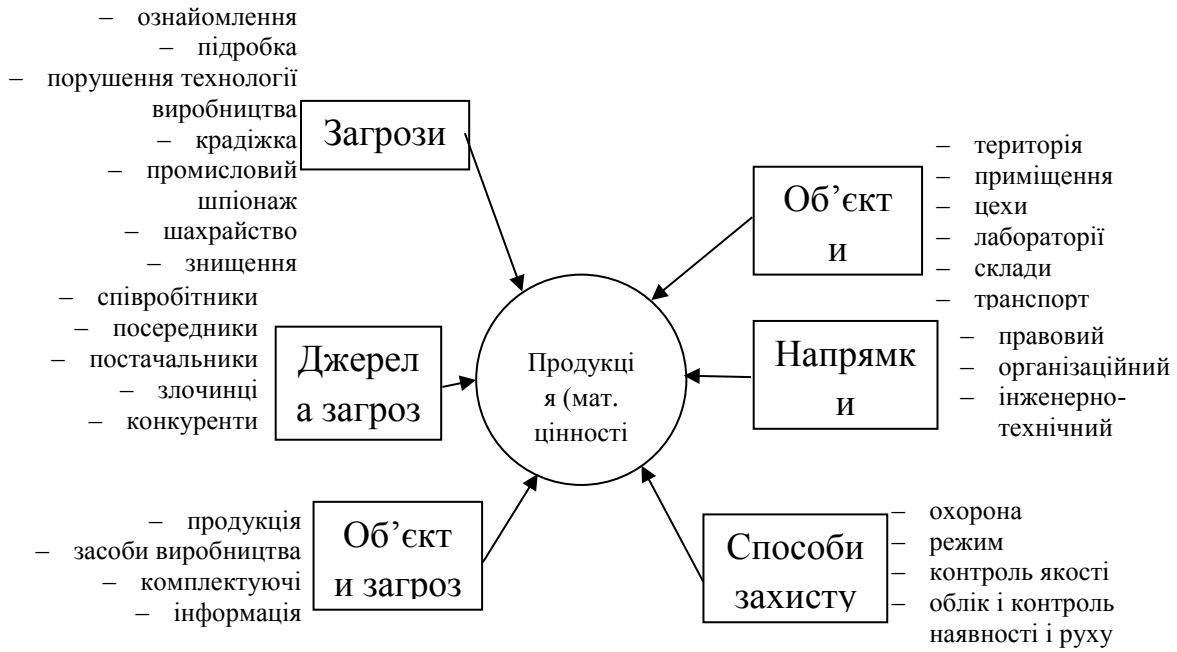

Рис. 20. Концептуальна модель безпеки продукції

Рис. 21. Концептуальна модель безпеки інформації.

Визначення основних принципів віднесення відомостей, що мають конфіденційний характер, до захищуваної інформації. Створенням

законодавчої бази в області інформаційної безпеки кожна держава прагне захистити свої інформаційні ресурси. Інформаційні ресурси держави у першому наближенні можуть бути розділені на три великі групи [xiv, xxiii]:

- ***відкрита інформація*** – на розповсюдження та використання такої інформації немає ніяких обмежень;
- ***запатентована інформація*** – охороняється внутрішньодержавним законодавством чи міжнародними угодами як об'єкт інтелектуальної власності;
- ***інформація, що захищається її власником*** – власник самостійно захищає цю інформацію з використанням відпрацьованих механізмів захисту державної, комерційної чи іншої таємниці; до цього виду зазвичай відносять інформацію, яка не відома іншим особам, яка або не може бути запатентована, або зумисно не патентується з метою уникнення чи зменшення ризику заволодіння нею суперниками та/чи конкурентами.

Захищають і охороняють, як правило, не всю, чи не всяку інформацію, а найважливішу, цінну для власника, обмеження розповсюдження якої приносить йому якусь користь чи прибуток, можливість ефективно вирішувати поставлені перед ним задачі. До захищуваної відносять наступні види інформації [xiv]:

- ***Секретну інформацію***. До секретної інформації відносять відомості, що містять державну таємницю.
- ***Конфіденційну інформацію***. До цього виду захищуваної інформації зазвичай відносять відомості, що містять комерційну таємницю, а також таємницю, що стосується особистого (не службового) життя та діяльності громадян.

Таким чином, під захищуваною інформацією розуміють відомості, на використання і розповсюдження яких введено обмеження їх власником і такі, що характеризуються поняттям „таємниця". Стосовно до органів державної влади та управління, під таємницею розуміють те, що приховується від інших, що відомо певному колу людей. Інакше кажучи, ті відомості, які не підлягають розголошенню, і є таємницею. Головний напрямок використання цього поняття – засекречування державою певних відомостей, приховування яких від суперників, потенційного противника дає їй можливість успішно вирішувати життєво важливі питання в області оборони країни, політичні, науково-технічні та інші проблеми з меншими затратами сил та засобів.

До подібного виду таємниці відноситься засекречування підприємством відомостей, які допомагають йому ефективно вирішувати задачі виробництва та вигідної реалізації продукції. Сюди ж відносяться і таємниці особистого життя громадян, які зазвичай охороняються державою: таємниця переписки, лікарська таємниця, таємниця грошового вкладу в банку тощо. Класифікацію інформації з точки зору її власника можна представити у вигляді таблиці (табл. 9).

Курсивом виділена та інформація, захист якої забезпечується державою.

Таблиця 9

Класифікація інформації стосовно її власника

Власник	**Вид інформації**				
	Захищаєма		**Запатентована**		**Відкрита**
	Секретна	**Конфі-денційна**	**Патент**	**Авторське право**	
Особа		– особиста таємниця; – персональні дані	*Патент фізичної особи*	*Авторське право фізичної особи*	
Суспільство		*Комерційна таємниця*	*Патент юридичної особи*	*Авторське право юридичної особи*	
Держава	*Державна таємниця*	*Службові відомості*	*Державний патент*		

Захищають та охороняють, як правило, не всю чи не всяку інформацію, а найважливішу, цінну для власника, обмеження розповсюдження якої приносить йому якусь користь чи прибуток, можливість ефективно вирішувати поставлені перед ним задачі. При цьому розрізняють ознаки захищуваної інформації [xiv]:

- засекречувати інформацію (обмежувати до неї доступ) може тільки її власник чи вповноважена на це власником особа;
- чим важливішою для власника є інформація, тим ретельніше він її захищає; а для того щоб усі, хто зіштовхується з цією захищуваною інформацією, знали, що одну інформацію слід зберігати ретельніше, ніж іншу, власник визначає їх різні ступені секретності;
- захищувана інформація повинна приносити певну користь її власнику і виправдовувати затрачені на її захист сили та засоби;
- секретна інформація володіє певною генетичною властивістю: якщо ця інформація є джерелом для створення нової інформації (документів, виробів тощо), то створена на її основі нова інформація, як правило, також є секретною.

Відмінною властивістю інформації, яка захищається, є те, що засекречувати її може тільки її власник чи уповноважені ним на те особи. Власниками захищуваної інформації можуть бути:

- ***держава та її структури (органи)***; в цьому випадку до неї відносяться відомості, які є державною, службовою таємницею, інші види захищуваної інформації, що належить державі чи відомству, до них можуть бути віднесені і відомості, які є комерційною таємницею;
- ***підприємства, товариства, акціонерні товариства та ін.*** – інформація є їх власністю та складає комерційну таємницю;

– ***громадяни держави*** (їх права – таємниця переписки, телефонних та телеграфних розмов, лікарська таємниця, персональні дані та ін. – гарантуються державою. Особисті таємниці – їх особиста справа; слід зазначити, що держава не несе відповідальності за збережуваність особистих таємниць).

Поняття „державна таємниця“ є одним із найважливіших у системі захисту державних секретів в будь-якій країні. Від його правильного визначення залежить і політика держави в області захисту секретів. Визначення цього поняття дається у Законі України „Про державну таємницю“ [xv]:

> ***Державна таємниця*** (також – ***секретна інформація***) – вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визначені у порядку, встановленому цим Законом, державною таємницею і підлягають охороні державою.

Модель визначення державних секретів зазвичай включає в себе наступні суттєві ознаки:

1. Предмети, явища, події, галузі діяльності, що складають державну таємницю.
2. Противник (наявний чи потенційний), від якого в основному здійснюється захист державної таємниці.
3. Вказування в законі, переліку, інструкції відомостей, що складають державну таємницю.
4. Завдані збитки обороні, зовнішній політиці, економіці, науково-технічному прогресу країни тощо у випадку розголошення відомостей, що складають державну таємницю.

Цим же Законом про державну таємницю визначено які відомості можуть бути віднесені до державної таємниці. До них відносяться відомості: у сфері оборони; у сфері економіки, науки і техніки; у сфері зовнішніх відносин а також у сфері державної безпеки та охорони правопорядку. Не можна засекречувати інформацію і надавати їй статус державної таємниці [xv]:

– якщо її втрата (розголошення та ін.) не приводить до збитків національній безпеці країни, порушення діючих законів;
– якщо приховування інформації буде порушувати конституційні та законодавчі права громадян;
– для приховування діяльності, що наносить збитки навколишньому природному середовищу, що загрожує життю та здоров’ю громадян.

Поняття, види та розмір збитків відрізняються для кожного конкретного об’єкту захисту – змісту відомостей, що складають державну таємницю,

сутності відображених у них фактів, подій, явищ дійсності. Залежно від виду, змісту та розмірів збитків можна виділити групи деяких видів збитків при втраті (чи можливій втраті) відомостей, що складають державну таємницю.

Політичні збитки можуть наступати при втраті відомостей політичного та зовнішньополітичного характеру, про розвідувальну діяльність спецслужб держави тощо. Політичні збитки можуть виражатися в тому, що у результаті втрати інформації можуть відбутися серйозні зміни в міжнародній обстановці не на користь України, втрата країною політичних пріоритетів в якихось областях, погіршення відносин з якоюсь країною чи групою країн тощо.

Економічні збитки можуть наступати при втраті відомостей будь-якого змісту: політичного, економічного, військового, науково-технічного і т.д. Економічні збитки можуть бути виражені в першу чергу в грошовому еквіваленті. Економічні збитки від втрати інформації можуть бути прямими та опосередкованими. Так, прямі втрати можуть наступити в результаті втрати секретної інформації про системи озброєнь, оборону країни, які в результаті цього втратили свою ефективність і потребують значних затрат на їх заміну чи переналагодження. Опосередковані втрати найчастіше виражаються у вигляді розміру втраченої вигоди: зрив переговорів з іноземними фірмами про вигідні угоди, за якими були укладені попередні домовленості; втрата пріоритету в науковому дослідженні, в результаті чого суперник швидше довів свої дослідження до завершення і запатентував їх і т.д.

Моральні збитки, як правило, нематеріального характеру наступають від втрати інформації, яка викликала чи ініціювала пропагандистську компанію, що підриває репутацію країни, привела до видворення з якихось країн наших дипломатів, розвідників, що діяли під дипломатичним прикриттям тощо.

Проблема засекречування інформації та визначення міри секретності відомостей, документів, виробів та робіт є однією із стержневих в усій діяльності із захисту інформації. Вона має велике державне значення, визначає методологію та методику захисту інформації, об’єми робіт з її захисту та інші обставини, зв’язані з діяльністю державних органів, підприємств та організацій в цій області. Правила засекречування інформації визначають в кінцевому рахунку політику держави в області захисту секретів. Цим і пояснюється, що переліки відомостей, які складають державну таємницю, затверджуються на найвищому рівні і у них відображається концепція керівництва країни в області захисту державних секретів.

Засекречувати інформацію мають право органи влади, управління та посадові особи, наділені відповідними повноваженнями [xv]. Вони:

- здійснюють політику держави в області захисту інформації;
- визначають категорії відомостей, що підлягають захисту та

засекречуванню, і закріплюють це в законодавчих актах;
- розробляють переліки відомостей, що підлягають засекречуванню;
- визначають міру секретності документів, виробів, робіт та відомостей і проставляють на носіях захищаємої інформації відповідні грифи секретності.

Таким чином,

засекречування інформації – це сукупність організаційно-правових заходів, регламентованих законами та іншими нормативними актами, по введенню обмежень на розповсюдження і використання інформації в інтересах її власника.

Окреслимо коротко основні принципи засекречування інформації.

1. ***Законність засекречування інформації***. Полягає у здійсненні засекречування строго в рамках діючих законів та інших підзаконних нормативних актів. Не виконання цього принципу може нанести серйозні збитки інтересам захисту інформації, інтересам особи, суспільства та держави, зокрема шляхом незаконного приховування від суспільства інформації, що не потребує засекречування чи у зв'язку із розголошенням важливої інформації.
2. ***Обгрунтованість засекречування інформації***. Полягає у встановленні шляхом експертної оцінки доцільності засекречування конкретних відомостей, ймовірних економічних чи інших наслідків цього акту, виходячи з балансу життєво важливих інтересів особи, суспільства та держави. Невиправдано засекречувати інформацію, ймовірність розкриття якої перевищує ймовірність зберігання її в таємниці.
3. ***Своєчасність засекречування інформації***. Полягає у встановленні обмежень на розповсюдження цих відомостей з моменту їх отримання (розробки) чи заздалегідь.
4. ***Підпорядкованість відомчих заходів із засекречування інформації загальнодержавним інтересам***. Це, в першу чергу, відноситься до області захисту державної таємниці. Що ж стосується комерційної таємниці, то підприємства наділені усіма правами засекречування інформації, крім обумовлених у законодавстві випадків.

Для забезпечення ефективного захисту інформації, що відноситься до державної таємниці, та здійснення єдиної державної політики в області засекречування інформації використовується „Перелік посадових осіб, на яких покладається виконання функцій державного експерта з питань таємниць" [xvi], затверджений Указом Президента від 29 травня 2006 року, № 452/2006 та „Звід відомостей, що становлять державну таємницю" [xvii], затверджений Службою безпеки України 12 серпня 2005 року, № 440.

Керівники (державні експерти), наділені повноваженнями із засекречування інформації, утверджують своїми наказами переліки відомостей, що підлягають засекречуванню, відповідно до їх галузевої, відомчої чи програмно-цільової належності. Вони ж наділяються повноваженнями розпоряджатися цими відомостями, перегляду міри їх секретності та розсекречування.

Міра секретності та конфіденційності інформації, відображеної у документах, виробах тощо не залишається постійною. Вона зазвичай зменшується і рідше (наприклад, документи представляють історичну чи іншу цінність), може збільшуватися. Міра секретності та конфіденційності інформації періодично повинна переглядатися. При цьому вона може бути збільшена, знижена чи взагалі може бути знято гриф секретності.

Розсекречування конфіденційної та секретної інформації, робіт, документів, виробів – це діяльність підприємств із зняття (частковому чи повному) обмежень на доступ до раніше засекреченої інформації, на доступ до її носіїв, викликана вимогами законодавства та об’єктивними факторами: зміною міжнародної та загальнодержавної обстановки, появою довершеніших видів певної техніки, зняттям виробів з виробництва, передачею (продажем) науково-технічних рішень оборонного характеру в народне господарство, продажем виробів за кордон і т.д., а також взяттям державою на себе міжнародних зобов’язань з відкритого обміну відомостями, які в Україні відносяться до державної таємниці. Інформація повинна залишатися секретною чи конфіденційною до того часу, поки цього вимагають інтереси національної безпеки чи конкурентної та комерційної діяльності підприємства.

Принципові аспекти розсекречування інформації можуть бути викладені в наступних основних положеннях:

1. Інформація не підлягає засекречуванню, а засекречена не повинна бути розсекреченою, якщо це зроблено необгрунтовано та в порушення діючих законів, з метою приховування порушень законності, в результаті невмілого керівництва та посадових помилок, порушення конституційних та інших законодавчих прав громадян.
2. Інформація розсекречується не пізніше термінів, встановлених при її засекречуванні. Раніше цих термінів підлягає розсекречуванню тільки інформація, що підпадає під дію взятих на себе Україною міжнародних зобов’язань з відкритого обміну інформацією. Термін засекречування інформації, віднесеної до державної таємниці не повинен перевищувати 30 років. Правом продовження термінів засекречування інформації наділяються керівники центральних органів виконавчої влади, які здійснили віднесення відповідних відомостей до державної таємниці.

3. Інформація не підлягає засекречуванню, а засекречена повинна бути розсекреченою, якщо вміщені в неї нові наукові, проектні, технологічні і т.п. розробки перебувають нижче світового технологічного рівня або досить детально висвітлені в зарубіжних чи вітчизняних публікаціях.
4. Розсекречуванню (розголошенню) не підлягають відомості, що зачіпляють особисте (не службове) життя громадян країни, якщо на протилежне немає згоди самих громадян, а у випадку їх смерті – їх найближчих родичів. Інший порядок такого розсекречування розглядається через суд.

2.3. Державна політика у сфері безпеки інформаційних ресурсів

Зростання децентралізації та розподіленої обробки даних, які все більше проявляються останнім часом, висунуло проблеми забезпечення безпеки інформації до числа найважливіших для національної економіки. Розв’язання проблеми забезпечення інформаційної безпеки передбачає комплекс заходів і, в першу чергу, такі дії держави, як розробка системи класифікації та документування інформації і способів захисту, регулювання доступу до даних та встановлення відповідальності за порушення інформаційної безпеки.

Державна політика у сфері формування інформаційних ресурсів повинна бути направлена на створення умов для ефективного і якісного інформаційного забезпечення розв’язання стратегічних і оперативних задач соціального і економічного розвитку країни. Головними напрямками державної політики у сфері інформатизації є [xviii]:

- забезпечення умов для розвитку і захисту усіх форм власності на інформаційні ресурси;
- формування та захист державних інформаційних ресурсів;
- створення та розвиток державних і регіональних інформаційних систем і мереж, забезпечення їх сумісності та взаємодії в єдиному інформаційному просторі;
- створення умов для якісного і ефективного інформаційного забезпечення громадян, органів державної влади, організацій та громадських об’єднань на основі державних інформаційних ресурсів;
- забезпечення національної безпеки у сфері інформатизації, а також забезпечення реалізації прав громадян та організацій в умовах інформатизації;
- сприяння формуванню ринку інформаційних ресурсів, послуг, інформаційних систем, технологій, засобів їх забезпечення;
- формування та здійснення єдиної науково-технічної та промислової політики у сфері інформатизації з врахуванням сучасного світового рівня

розвитку інформаційних технологій;

- підтримка проектів та програм інформатизації;
- створення та удосконалення системи залучення інвестицій та механізму стимулювання розробки і реалізації проектів інформатизації;
- розвиток законодавства у сфері інформаційних процесів, інформатизації та захисту інформації.

Обов'язковою умовою включення інформації до інформаційних ресурсів є ***документування інформації***. Документування здійснюється у порядку, який встановлюється органами державної влади, відповідальними за організацію діловодства, стандартизацію документів та їх масивів.

Документ, отриманий із інформаційної системи, набуває юридичної сили після його підписання посадовою особою в порядку, встановленому законом. Юридична сила документу, який зберігається, обробляється та передається за допомогою автоматизованих інформаційних та телекомунікаційних систем, може підтверджуватися електронним цифровим підписом. Юридична сила електронного цифрового підпису визнається за наявності у інформаційній системі програмно-технічних засобів, що забезпечують ідентифікацію підпису, та дотримання встановленого режиму їх використання [xix]. Право посвідчувати ідентичність електронного цифрового підпису здійснюється на основі ліцензії.

Інформаційні ресурси можуть бути державними і недержавними, і як елемент складу майна можуть бути у власності громадян, органів влади, організацій та громадських об'єднань. Відношення з приводу права власності на інформаційні ресурси регулюється відповідним цивільним законодавством [xx]. Фізичні та юридичні особи є власниками тих документів, масивів документів, які створені на їх кошти, куплені ними на законних засадах, отримані шляхом дарування чи спадкування.

Держава має право викупу документованої інформації у фізичних та юридичних осіб у випадку віднесення цієї інформації до державної таємниці [xv]. Власник інформаційних ресурсів, які містять відомості, віднесені до державної таємниці, має право розпоряджатися цією власністю тільки з дозволу відповідних органів державної влади. Суб'єкти, які надають в обов'язковому порядку документовану інформацію до органів державної влади не втрачають своїх прав на ці документи та на використання інформації, що міститься у них. Документована інформація, яка надається в обов'язковому порядку до органів державної влади та організації юридичними і фізичними особами формує інформаційні ресурси, що перебувають у спільному володінні держави та суб'єктів, що надають цю інформацію.

Інформаційні ресурси можуть бути товаром, за виключенням випадків,

передбачених відповідним законодавством [xiv]. Право власності на засоби обробки інформації не створює права власності на інформаційні ресурси, що належать іншим власникам. Документи, що обробляються в порядку надання послуг чи при спільному використанні цих засобів обробки, належать їх власнику. Належність і режим похідної продукції, що створюється в цьому випадку, регулюється договором.

Формування державних інформаційних ресурсів здійснюється громадянами, органами державної влади, органами місцевого самоуправління, організаціями та громадськими об'єднаннями. Документи, що належать фізичним і юридичним особам, можуть бути включені за бажанням власника до складу державних інформаційних ресурсів за правилами, встановленими для включення документів до відповідних інформаційних систем. Державні інформаційні ресурси є відкритими і загальнодоступними. Виключення складає документована інформація, віднесена законом до категорії обмеженого доступу. Документована інформація з обмеженим доступом за умовами її правового режиму поділяється на інформацію, віднесену до державної таємниці та конфіденційну інформацію.

Персональні дані відносяться до категорії конфіденційної інформації [xiv]. Не допускається збирання, зберігання та розповсюдження інформації про приватне життя, а також інформації, яка порушує особисту чи сімейну таємницю, таємницю переписки, телефонних переговорів, поштових, телеграфних та інших повідомлень особи без її згоди, за виключенням випадку наявності рішення суду. Персональні дані не можуть бути використані з метою нанесення майнової та моральної шкоди громадянам, ускладнення реалізації їх прав та свобод. Обмеження прав громадян на основі використання інформації про їх соціальне походження, расову, національну, мовну, релігійну та партійну належність заборонено і карається відповідно до закону.

Юридичні та фізичні особи, які, відповідно до своїх повноважень, володіють інформацією про громадян, отримують та використовують її, відповідно до закону несуть відповідальність за порушення режиму захисту, обробки і порядку використання цієї інформації. При вирішенні правових питань у процесі впровадження сучасних інформаційних технологій не можна забувати про можливі порушення законних прав та інтересів громадян шляхом недобросовісної поведінки користувачів таких систем, наприклад при несанкціонованому використанні інформації чи її зумисному спотворенні.

Розуміється, що тенденція до розширення числа видів інформації про особу, які накопичуються у банках даних, носить об'єктивний характер і зумовлена зростанням ролі інформації у вирішенні масштабних виробничих та соціально-культурних задач. Проте очевидно, що об'єм зібраних даних повинен

бути обмеженим, по-перше, тільки найнеобхіднішими відомостями і, по-друге, реальна можливість нанесення шкоди законним інтересам громадян, про яких збирається така інформація, повинна виключати збирання такої інформації. Адже поява великих електронних інформаційних систем, що накопичують великі масиви відомостей такого типу, дозволяє створювати образ людини і розробляти відповідну систему контролю за нею. У результаті ставиться під сумнів принцип „презумпції невинності“, оскільки людина, за якою ведеться спостереження незаконно, без її відома, потрапляє в становище підозрюваного чи навіть звинувачуваного.

У плані взаємозв’язку забезпечення і законності реалізації прав і свобод громадян прийнято закони [xiv,xxi], які дозволяють громадянам, засобам масової інформації та приватним організаціям знайомитися з інформацією урядових закладів. Право громадян затребувати інформацію стосується документації усіх органів влади: міністерств, адміністративних та військових відомств, державних підприємств та інших закладів. Під дію цих законів не підпадає документація, що відноситься до державної таємниці [xv]. У тих випадках, коли використання інформації може потягнути позбавлення громадянина прав, пільг та привілеїв заклад повинен по можливості отримувати інформацію безпосередньо від особи.

Користувачі – громадяни, органи державної влади, органи місцевого самоуправління, організації та громадські об’єднання – мають рівні права на доступ до державних інформаційних ресурсів і не зобов’язані обґрунтовувати перед власником цих ресурсів необхідність отримання цієї інформації. Виключення складає інформація з обмеженим доступом. Доступ фізичних і юридичних осіб до державних інформаційних ресурсів є основою здійснення громадського контролю за діяльністю органів державної влади, органів місцевого самоуправління, громадських, політичних чи інших організацій, а також за станом економіки, екології та інших сфер громадського життя.

Інформація, отримана на законних підставах із державних інформаційних ресурсів громадянами і організаціями, може бути ними використана для створення довільної інформації з метою її комерційного розповсюдження з обов’язковим посиланням на джерело інформації. Джерелом прибутку в цьому випадку є результат праці та вкладених засобів при створенні довільної інформації, але джерелом прибутку при цьому не може бути вихідна інформація.

Порядок накопичення і обробки документованої інформації з обмеженим доступом, правила її захисту і порядок доступу до неї визначається органами державної влади, відповідальними за певні масиви та види інформації, відповідно до їх компетенції, або безпосередньо її власником, відповідно до

законодавства.

Громадяни та організації мають право на доступ до документованої інформації про них, на уточнення цієї інформації з метою забезпечення її повноти та достовірності, мають право знати хто і з якою метою використовує чи використовував цю інформацію. Обмеження доступу громадян та організацій до інформації про них допустиме тільки у випадках, передбачених законом [xiv,xv]. Власник інформаційних ресурсів зобов'язаний забезпечити дотримання режиму обробки та правил надання інформації користувачу, встановлених законодавством, чи власником цих інформаційних ресурсів, відповідно до законодавства. Власник інформаційних ресурсів несе юридичну відповідальність за порушення правил роботи з інформацією в порядку, передбаченому відповідним законодавством.

Усі види виробництва інформаційних систем, технологій та засобів їх забезпечення складають спеціальну галузь економічної діяльності. Державні і недержавні організації та громадяни мають рівні права на розробку і виробництво інформаційних систем, технологій та засобів їх забезпечення. Інформаційні системи, технології і засоби їх забезпечення можуть бути об'єктами власності фізичних і юридичних осіб та держави. Власником інформаційної системи, технології та засобів їх забезпечення визнається фізична чи юридична особа, на кошти якої ці об'єкти виготовлені, придбані чи отримані в порядку наслідування, дарування чи іншим законним способом. Інформаційні системи, технології та засоби їх забезпечення виступають у якості товару (продукції) при дотриманні виключних прав їх розробників, а їх власник визначає умови їх розповсюдження.

Право авторства і право власності на інформаційні системи, технології та засоби їх забезпечення можуть належати різним особам. Власник інформаційної системи, технології та засобів їх забезпечення зобов'язаний захищати права їх автора відповідно до законодавства.

Інформаційні системи, бази і банки даних, призначені для інформаційного обслуговування громадян і організацій необхідно сертифікувати у встановленому порядку. Організації, що виконують роботи в області проектування, виробництва засобів захисту та обробки персональних даних, отримують ліцензії на цей вид діяльності. Порядок ліцензування визначається відповідним законодавством [xxii].

2.4. Правовий захист інформації в інформаційних системах

Сам по собі факт призначення обчислювальної системи для широкого кола користувачів створює певний ризик у плані безпеки, оскільки не всі

клієнти будуть виконувати вимоги з її забезпечення. Порядок зберігання носіїв інформації повинен бути чітко визначеним у відповідному правовому акті і передбачати збережуваність носіїв інформації, контроль за роботою з інформацією, відповідальність за несанкціонований доступ до носіїв інформації з метою зняття з них копій, зміни чи пошкодження.

В інформаційних системах є можливість приховано отримати доступ до інформаційних архівів, що концентруються в одному місці у великих об'ємах. Крім того, з'явилася можливість дистанційного отримання інформації. Тому для захисту інформації використовуються принципово нові методи та засоби, розроблені із врахуванням цінності інформації, умов роботи, технічних та програмних можливостей ЕОМ та інших засобів збирання, передачі та обробки даних. Особливі захисні міри необхідні у випадках, коли ресурси ЕОМ використовуються кількома користувачами в багатопрограмному режимі та режимі розділення часу. Тут виникає ряд правових проблем, пов'язаних з масивами інформації, які представляють собою суспільну та національну цінність, а їх зміст – національну таємницю. Використання такої інформації не за призначенням може привести до значних збитків як суспільству в цілому, так і окремій особі.

Окремо слід звернути увагу на правові аспекти захисту інформації, які можуть виникнути при недостатньо продуманому чи зловмисному використанні електронно-обчислювальної техніки. До них відносяться:

1. Правові питання захисту масивів інформації від спотворень та встановлення юридичної відповідальності за порушення збереженості інформації.
2. Юридичні та технічні питання захисту інформації від несанкціонованого доступу до неї, які виключають можливість неправомірного її використання.
3. Встановлення юридично закріплених норм та методів захисту авторських прав та пріоритетів розробників програмного продукту.
4. Розробка заходів з надання юридичної сили електронним документам та засобів, які перешкоджають фальсифікації таких документів.
5. Правовий захист інтересів експертів, які передають свої знання до фондів банків даних.
6. Встановлення правових норм та юридичної відповідальності за використання електронно-обчислювальних засобів в особистих цілях, що суперечать інтересам інших осіб та суспільства і можуть завдати їм шкоду

Відсутність належної реєстрації та контролю робіт, низька трудова і виробнича дисципліна персоналу, доступ посторонніх осіб до обчислювальних ресурсів створюють умови для зловживань і ускладнюють їх виявлення. У

кожному обчислювальному центрі прийнято встановлювати та строго дотримуватися регламенту доступу в різні службові приміщення для різних категорій співробітників. Ступінь захисту інформації від неправомірного доступу та протизаконних дій залежить від якості розробки організаційних заходів, направлених на унеможливлення [xxiii,xxiv]:

- доступу сторонніх до апаратури обробки інформації;
- безконтрольного виносу персоналом різноманітних носіїв інформації;
- несанкціонованого введення даних в пам'ять, зміни чи витирання інформації, що зберігається в пам'яті;
- незаконного користування системами обробки інформації та отриманими даними;
- доступу до систем обробки інформації з використанням саморобних пристроїв;
- несанкціонована передача даних по каналах зв'язку із інформаційно-обчислювального центру;
- безконтрольне введення даних в систему;
- обробка даних без відповідної вимоги замовника;
- несанкціоноване зчитування, зміна чи знищення даних в процесі їх передачі чи транспортування носіїв інформації.

Метою захисту інформації є [xxiv]:

- запобігання витоку, викраденню, втраті, спотворенню, підробці інформації;
- запобігання загрозам безпеки особи, суспільства, держави;
- запобігання несанкціонованим діям по знищенню, модифікації, спотворенню, копіюванню, блокуванню інформації;
- запобігання іншим формам незаконного втручання в інформаційні ресурси та інформаційні системи;
- забезпечення правового режиму документованої інформації, як об'єкта власності;
- захист конституційних прав громадян на зберігання особистої таємниці та конфіденційності персональних даних, доступних в інформаційних системах;
- зберігання державної таємниці, конфіденційності документованої інформації відповідно до законодавства;
- гарантування прав суб'єктів в інформаційних процесах та при розробці, виробництві і використанні інформаційних систем, технологій та засобів їх забезпечення.

Захисту підлягає будь-яка документована інформація, неправомірне використання якої може нанести збитки її власнику, користувачу чи іншій

особі. Контроль за дотриманням вимог до захисту інформації та експлуатації спеціальних програмно-технічних засобів захисту, а також забезпечення організаційних мір захисту інформаційних систем, що обробляють інформацію з обмеженим доступом в недержавних структурах, здійснюється органами державної влади. Організації, що працюють з інформацією з обмеженим доступом, яка є власністю держави, створюють спеціальні служби, які забезпечують захист інформації.

Власник документу, масиву документів, інформаційних систем забезпечує рівень захисту інформації відповідно до законодавства. Власник інформаційних ресурсів чи уповноважені ним особи мають право здійснювати контроль за виконанням вимог із захисту інформації та забороняти чи призупиняти обробку інформації у випадку невиконання цих вимог. Власник документованої інформації має право звертатися до органів державної влади для оцінки правильності виконання норм і вимог із захисту його інформації в інформаційних системах. Власник інформаційних ресурсів чи уповноважені ним особи відповідно до закону встановлюють порядок надання користувачу інформації із вказуванням місця, часу, відповідальних посадових осіб а також необхідних процедур і забезпечують необхідні умови доступу користувачів до інформації.

Ризик, пов’язаний із використанням не сертифікованих інформаційних систем і засобів їх забезпечення лежить на власнику цих систем і засобів. Ризик, пов’язаний з використанням інформації, отриманої із не сертифікованої системи, лежить на споживачі інформації.

Відповідальність за порушення міжнародних норм і правил в галузі формування та використання інформаційних ресурсів, створення та використання інформаційних систем, технологій та засобів їх забезпечення покладається на органи державної влади, організації і на громадян відповідно до договорів, укладених ними із закордонними фірмами та іншими партнерами із врахуванням міжнародних договорів.

Відмова в доступі до відкритої інформації чи надання користувачам завідомо недостовірної інформації можуть бути оскаржені в судовому порядку. Керівники та співробітники органів державної влади і організацій, винні у незаконному обмеженні доступу до інформації та порушенні режиму захисту інформації, несуть відповідальність відповідно до чинного кримінального, адміністративного та цивільного законодавства.

Державна система правового забезпечення захисту інформації в інформаційних системах. Другою функцією організаційно-правового забезпечення інформаційної безпеки є визначення системи органів та посадових осіб, відповідальних за забезпечення інформаційної безпеки в країні. Основою

для створення державної системи організаційно-правового забезпечення захисту інформації є створювана в даний час державна система захисту інформації, під якою розуміється сукупність державних та інших органів управління і взаємозв'язаних правових, організаційних та технічних заходів, здійснюваних на різних рівнях управління та реалізації інформаційних відношень і направлених на забезпечення безпеки інформаційних ресурсів.

Під інформаційною безпекою України розуміється стан захищеності її національних інтересів в інформаційній сфері, який визначається сукупністю збалансованих інтересів особи, суспільства та держави.

Нагадаємо зміст інтересів особи, суспільства та держави в інформаційній сфері. Інтереси особи в інформаційній сфері полягають у реалізації конституційних прав людини на доступ до інформації, на використання інформації в інтересах здійснення не забороненої законом діяльності, фізичного, духовного та інтелектуального розвитку, а також у захисті інформації, що забезпечує особисту безпеку.

Інтереси суспільства в інформаційній сфері полягають у забезпеченні інтересів особи в цій сфері, укріпленні демократії, створенні правової соціальної держави, досягненні та підтримці суспільної згоди, в духовному оновленні України.

Інтереси держави в інформаційній сфері полягають у створенні умов для гармонійного розвитку української інформаційної інфраструктури, для реалізації конституційних прав людини в області отримання інформації та користування нею в цілях забезпечення непорушності конституційного ладу, суверенітету та територіальної цілісності України, політичної, економічної та соціальної стабільності, в безумовному забезпеченні законності та правопорядку, розвитку рівноправного та взаємовигідного міжнародного співробітництва. На основі національних інтересів України в інформаційній сфері формуються стратегічні та поточні задачі внутрішньої та зовнішньої політики держави із забезпечення інформаційної безпеки.

Проаналізуємо компетенцію органів державної влади, органів місцевого самоврядування та їх посадових осіб у сфері державної таємниці та інформаційної безпеки, яка регулюється Законом України „Про державну таємницю" №3855-XII від 21 січня 1994 року [xv] (останні зміни до цього Закону датовані 21 травня 2008 року). Президент України, забезпечуючи національну безпеку, видає укази та розпорядження з питань охорони державної таємниці, віднесених до його повноважень. Рада Національної безпеки і оборони України координує та контролює діяльність органів виконавчої влади у сфері охорони державної таємниці. Кабінет Міністрів України спрямовує та координує діяльність органів виконавчої влади у сфері

охорони державної таємниці. Центральні та місцеві органи виконавчої влади, Рада міністрів Автономної Республіки Крим та органи місцевого самоврядування здійснюють державну політику у сфері охорони державної таємниці в межах своїх повноважень. Спеціально уповноваженим органом державної влади у сфері забезпечення охорони державної таємниці є Служба безпеки України. Забезпечення охорони державної таємниці відповідно до вимог режиму секретності в органах державної влади, органах місцевого самоврядування, на підприємствах, в установах і організаціях, діяльність яких пов'язана з державною таємницею, покладається на керівників зазначених органів, підприємств, установ і організацій.

Служба безпеки України координує роботу із [xv]:

1) забезпечення безпеки інформації в системах інформаційної та телекомунікаційної інфраструктури, які мають значний вплив на безпеку держави в інформаційній сфері;
2) протидії іноземним технічним розвідкам на території України;
3) забезпечення захисту (некриптографічними методами) інформації, що містить відомості, які віднесені до державної таємниці, іншої інформації з обмеженим доступом, запобігання витіканню інформації по технічним каналам, несанкціонованого доступу до неї, спеціальних впливів на інформацію (носії інформації) з метою її зчитування, знищення, спотворення та блокування доступу до неї на території України;
4) захисту інформації при розробці, виробництві, експлуатації та утилізації неінформаційних випромінюючих комплексів, систем та пристроїв.

Основними задачами в галузі забезпечення інформаційної безпеки для Служби безпеки України є [xv]:

1) реалізація у межах своєї компетенції державної політики в галузі забезпечення безпеки інформації в ключових системах інформаційної інфраструктури, протидія технічним розвідкам та технічний захист інформації;
2) здійснення державної науково-технічної політики в галузі захисту інформації при розробці, виробництві, експлуатації та утилізації інформаційних випромінюючих комплексів, систем та пристроїв;
3) організація діяльності державної системи протидії технічним розвідкам та технічного захисту інформації на державному, міжрегіональному, регіональному, галузевому та об'єктовому рівнях;
4) забезпечення в межах своєї компетенції безпеки інформації в ключових системах інформаційної інфраструктури, протидія технічним розвідкам та технічний захист інформації в органах державної влади, органах місцевого самоуправління та організаціях;

5) прогнозування розвитку сил, засобів та можливостей технічних розвідок, виявлення загроз безпеці інформації;
6) протидія добуванню інформації технічними розвідувальними засобами, технічний захист інформації;
7) здійснення координації діяльності державних органів виконавчої влади та організацій з державного регулювання розміщення та використання іноземних технічних засобів спостереження та контролю в ході реалізації міждержавних угод, інших програм та проектів на території України.

Інші органи державного управління в межах своєї компетенції [xiv]:

1) визначають перелік відомостей, що підлягають охороні;
2) забезпечують розробку та здійснення технічних мір із захисту інформації на підвідомчих підприємствах;
3) організовують та координують проведення досліджень в галузі захисту інформації відповідно до державних програм;
4) розробляють галузеві документи з захисту інформації;
5) контролюють виконання на галузевих підприємствах встановлених норм та вимог із захисту інформації;
6) створюють галузеві центри з захисту інформації та контролю ефективності вжитих заходів;
7) організовують підготовку та підвищення кваліфікації фахівців із захисту інформації.

Для забезпечення виконання вказаних функцій до складу органів державного управління включаються науково-технічні підрозділи захисту інформації та контролю. На підприємствах, що виконують оборонні та інші секретні роботи, функціонують науково-технічні підрозділи захисту інформації та контролю, що контролюють діяльність в цьому напрямку наукових та виробничих структурних підрозділів підприємства, приймають участь в розробці і реалізації заходів із захисту інформації, здійснюють контроль ефективності цих заходів.

Крім того, в галузях промисловості та в регіонах країни створюються і функціонують ліцензійні центри, що здійснюють реалізацію і контроль за ліцензійною діяльністю в галузі надання послуг із захисту інформації, органи по сертифікації засобів обчислювальної техніки та засобів зв'язку, випробовувальні центри по сертифікації конкретних видів продукції на предмет безпеки інформації, органи з атестації об'єктів інформатики.

Державна система забезпечення інформаційної безпеки призначена для розв'язання наступних проблем, що вимагають законодавчої підтримки:

1) захист персональних даних;
2) боротьба з комп'ютерною злочинністю, насамперед у фінансовій сфері;

3) захист комерційної таємниці та забезпечення сприятливих умов для підприємницької діяльності;
4) захист державних секретів;
5) створення системи взаємних фінансових розрахунків в електронній формі з елементами цифрового підпису;
6) забезпечення безпеки автоматизованих та автоматичних систем управління потенційно небезпечних виробництв;
7) страхування інформації та інформаційних систем;
8) сертифікація та ліцензування в галузі безпеки, контроль безпеки інформаційних систем;
9) організація взаємодії у сфері захисту даних з іншими державами.

Структура нормативної бази з питань інформаційної безпеки включає:

– Конституцію України [xxv];
– Закони України;
– кодекси України (кримінальний [xxvi], цивільний [xx], господарський [xxvii]);
– укази Президента України та постанови Кабінету Міністрів України;
– відомчі нормативні акти, державні стандарти, інші нормативні документи.

Серед законів слід відмітити наступні:

– „Про інформацію“ [xiv];
– „Про державну таємницю“ [xv];
– „Про ліцензування певних видів господарської діяльності“ [xxii];
– „Про захист інформації в інформаційно-телекомунікаційних системах“ [xxiii];
– „Про телекомунікації“ [xxviii];
– „Про Службу безпеки України“ [xxix];
– „Про електронний цифровий підпис“ [xix].

2.5. Законодавство із захисту інформаційних технологій

Українським кримінальним та адміністративним законодавством передбачена відповідальність за здійснення злочинів та правопорушень при роботі з документацією, вираженою документально. Досить детально розроблено питання встановлення відповідальності за розголошення відомостей, що складають державну таємницю.

Існуюче законодавство дозволяє класифікувати та встановлювати відповідальність за різні форми злочинів і правопорушень, зв’язаних з інформацією, представленою у вигляді відомостей чи документів. До них відносяться [xxvi]:

- особливо небезпечні державні злочини (зрада Батьківщині, шпигунство, диверсія, розголошення державної таємниці, втрата документів, що вміщують державну чи службову таємницю);
- корисливі злочини (крадіжка, привласнення, підробка, …);
- злочини, здійснені з необережності чи халатності (знищення, пошкодження, втрата);
- господарські злочини (випуск недоброякісної продукції).

Обробка інформації з використанням нових інформаційних технологій має ряд суттєвих особливостей. До них відносяться:

- існування інформації і програм у вигляді нематеріальної „електронної копії“;
- можливість необмеженого, прихованого та безслідного доступу сторонніх осіб до „електронної копії“ інформації і програм з метою їх крадіжки (копіювання), модифікації чи знищення;
- можливість введення в ЕОМ не обумовлених технологією програмних засобів, в тому числі і вірусного характеру, що саме по собі являє серйозну загрозу.

Для вирішення задачі встановлення відповідальності за зловживання з використанням комп’ютерної техніки потрібно:

1. Розповсюдити на інформацію та програми для ЕОМ, представлені у формі „Електронної копії“, властивості об’єкту майнового права (визнати їх об’єктом права власності та товарним продуктом).
2. Встановити правовий режим інформації, який передбачає обов’язкове її документування (як механізм визнання інформації об’єктом права власності).
3. Визнати протиправними зумисні дії, що підпадають під категорії „порушення норм захисту“, „крадіжка“ (копіювання), „несанкціонований доступ“, а також „розповсюдження комп’ютерних вірусів“ не залежно від наслідків, до яких вони привели.
4. Встановити відповідальність адміністрації за неприйняття заходів безпеки, що привело до здійснення комп’ютерного злочину.

Аналіз суб’єктів інформаційних відносин показує, що серед них виділяються наступні категорії осіб:

- власники інформаційних систем;
- персонал інформаційних систем;
- власники інформації;
- джерела інформації;
- користувачі;
- сторонні особи.

У сфері традиційної обробки інформації усі вказані категорії можна розділити на дві групи: особи, яким дозволено доступ до інформації, та особи, яким такий доступ не дозволений. Правопорушення та злочини можуть бути здійснені:

- по необережності (некомпетентності);
- по халатності;
- зумисно.

При класифікації правопорушень та злочинів слід керуватися також: їх високою громадською небезпекою, що вимагає класифікувати навіть ті дії, які не нанесли збитків, але створили передумови для їх нанесення (порушення технології обробки, порушення норм захищеності, неприйняття потрібних мір з організації захисту). При цьому збитки від злочину можуть виражатися у формі:

- втраченої вигоди;
- прямих фінансових втрат;
- моральних збитків.

Іноді задача оцінки інформації у вартісному виразі є надто проблематичною і часто напряму не може бути розв’язана, наприклад при виникненні загроз інформаційним системам, що обробляють секретну інформацію. В цьому випадку відповідальність встановлюється по аналогії до діючих норм кримінального права.

В цілому можна виділити такі критерії складу злочину в галузі обробки інформації:

1. Порушення правил реєстрації інформаційних систем та переліків оброблюваної інформації.
2. Порушення правил збору інформації, а саме: отримання інформації без дозволу та збір її понад дозволеного переліку.
3. Зберігання персональної інформації понад встановленого терміну.
4. Неналежне зберігання інформації.
5. Передача третім особам відомостей, які є комерційною таємницею, чи персональних відомостей.
6. Несвоєчасне інформування населення про події, явища і факти, які можуть нанести шкоду їх здоров’ю чи нанести матеріальні збитки.
7. Перевищення меж компетенції облікової діяльності, допущення неповних облікових записів і фальсифікації даних.
8. Умисне надання зацікавленим особам неточної інформації.
9. Порушення встановленого порядку забезпечення безпеки інформації.
10. Порушення правил і технології безпечної обробки інформації.
11. Порушення норм захищеності інформації, встановлених законом.
12. Порушення правил доступу до інформації чи до технічних засобів.

13. Порушення механізму захисту інформації та проникнення в систему.
14. Обхід засобів захисту та проникнення в систему.
15. Крадіжка інформації з використанням:
    15.1. технічних засобів;
    15.2. доступу до носіїв інформації.
16. Несанкціоноване знищення даних в інформаційних системах.
17. Несанкціонована модифікація даних в інформаційних системах.
18. Спотворення (модифікація) програмного забезпечення.
19. Перехоплення електромагнітних, акустичних чи оптичних випромінювань.
20. Перехоплення інформації, що передається по лініях зв'язку шляхом дистанційного підключення до них чи будь-якими іншими відомими способами.
21. Виготовлення та розповсбдження завідомо непридатного програмного забезпечення.
22. Розповсюдження комп'ютерних вірусів.
23. Розголошення парольно-ключової інформації.
24. Несанкціоноване ознайомлення (спроба) із захищеними даними.
25. Несанкціоноване копіювання (крадіжка).
26. Внесення в програмне середовище не обумовлених змін, в тому числі і вірусного характеру.

2.6. Правовий захист програмного забезпечення

Правовий захист програмного забезпечення за своєю проблематикою багато в чому співпадає з більш широкою задачею – правовим захистом інтелектуальної власності. На даний час є п'ять основних правових механізмів захисту програмного забезпечення [ii]:

- авторське право;
- патентне право;
- право промислових таємниць;
- право, що відноситься до недобросовісних методів конкуренції;
- контрактне право.

Два основних гравці на цій арені – ***авторське*** та ***патентне право***. Три останніх механізми часто об'єднують в одну групу. Термін дії патентів зазвичай є меншим часу існування програмних продуктів, у зв'язку з чим їх рідко використовують для захисту програмного забезпечення, у зв'язку з чим основним механізмом захисту програмного забезпечення є авторське право.

Основні положення авторського права встановлюють баланс між суспільним інтересом та захистом прав автора. З одного боку суспільство

потребує наукових робіт в ім’я процвітання, а з іншого – права автора повинні бути захищеними для того, щоб заохотити його до подальшої роботи. Таке балансування може забезпечити тільки добре продумане законодавство. Встановлено дві основні вимоги до „твору“, необхідні для його захисту авторським правом: оригінальність та реалізація в матеріальній формі. Тут, проте, виникає питання про єдиність представлення ідеї, точніше про запас можливих представлень ідеї. Якщо ідея представляється єдиним вираженням, то його захист рівносильний забороні використання такої ідеї, і не може захищатися авторським правом. Тому повинна бути встановлена деяка межа, починаючи з якої „твір“ захищається авторським правом. Це є особливо актуальним по відношенню до програм. Наприклад, асемблерна програма множення двох чисел з фіксованою комою навряд чи може бути захищена авторським правом. Правове визначення межі, починаючи з якої програми захищаються авторським правом, представляє собою дуже складну, а іноді й нерозв’язну задачу.

Авторське право забезпечує автоматичний захист. Захист авторським правом виникає разом зі створенням „твору“ незалежно від того, чи надав автор копію „твору“ в Бюро з авторського права для реєстрації. Однак без реєстрації власник авторського права не може реалізувати свої права. Наприклад він не може подати до суду для захисту його прав і не може отримати компенсацію.

Закон [xxiii] детально оговорює в якому вигляді повинні надаватися копії програм чи баз даних для їх реєстрації. У випадку опублікованої чи не опублікованої програми потрібно надати один екземпляр „ідентифікуючої порції“ програми, відтвореної у формі, яку можна візуально сприймати без допомоги комп’ютера чи іншого пристрою, на папері чи мікроформі. Після встановлення, що наданий твір можна захищати авторським правом та аналізу супроводжуючих документів, вимога реєструється і автору видається свідоцтво про реєстрацію.

Авторське право захищає твір від копіювання, але не забороняє незалежного створення еквівалентів. Таким чином, ризик монополізації знання при використанні авторського права є значно меншим, ніж при використанні патентного права і, як наслідок, стандарти захисту авторським правом не наскільки строгі, як стандарти захисту патентним правом. Авторське право надає автору наступні п’ять прав [xxx]:

- відтворення;
- підготовка похідних творів;
- розповсюдження копій;
- публічне відтворення;
- виставка.

Авторське право, як уже говорилося, захищає не ідею, а її вираження, конкретну форму представлення. Тому в основу захисту програм авторським правом покладено наступні поняття [xxx]:

Послідовність команд. Програма – це послідовність команд, у зв'язку з чим вона може розглядатися як „вираження" ідеї автора, як його твір.

Копіювання. Це поняття, що використовується у авторському праві, може бути розповсюджене на перенесення програм з одного носія на інший, в тому числі на носій іншого типу. Робити висновок про ідентичність програм на різних носіях можна за багатьма ознаками, наприклад, за їх однаковими функціональними властивостями, але співпадання функціональних властивостей не захищається авторським правом, адже однаковість функціональних властивостей іще не свідчить про відтворення „форми" (про копіювання).

Творча активність. Подібно до інших форм відображення, які захищаються авторським правом, комп'ютерна програма є результатом творчості. Хоча ця форма вираження чи відображення все ще не є загальновідомою, рівень творчої активності, умілості та винахідливості, необхідний для створення програми, дозволяє стверджувати, що програми підлягають захисту авторським правом не менше, ніж будь-які інші твори, що захищаються ним. Той факт, що комп'ютерні програми мають практичне призначення, на це не впливає.

Стиль. Творчість, уміліст та винахідливість автора проявляються в тому, як створюється програма. Необхідно поставити задачі, які потрібно розв'язати. Потім проаналізувати як досягти розв'язку, сформулювати набір кроків, що ведуть до розв'язання – все це повинно бути зафіксоване написанням тексту програми. Спосіб, яким це все досягається, надає програмі її характерні особливості і навіть стиль.

Алгоритм. Алгоритми – це, власне, кроки, з яких складається розв'язання задачі, що представляють собою елементи, з яких будується програма і які не можуть захищатися від неавторизованого використання авторським правом. Це аналоги слів у літературі чи мазків пензлем у живопису.

Відбір та поєднання елементів. Як і у випадку інших творів, захист комп'ютерних програм розглядається з точки зору відбору та об'єднання автором базових елементів, в чому і проявляється його творчість та вміліст, що і відрізняє його твір від творів інших авторів. Випадок, коли два автори незалежно один від одного написали б для однієї й тієї ж задачі дві ідентичні програми, практично виключений. Однак елементи, якими користуються автори, в основному загальновідомі.

Оригінальність програми. Основна вимога авторського права базується

на оригінальності відбору і поєднання загальновідомих елементів.

Успішність. Успіх у розв'язанні задачі у значній мірі визначається тим відбором та поєднанням елементів, який автор здійснив на кожному кроці створення програми. Тому програма може працювати швидше, бути простішою та надійнішою у використанні, легше сприйматися і бути більш продуктивною ніж її попередники чи конкуренти.

Усі ці та ряд інших міркувань і покладено в основу захисту програм авторським правом.

---

i. Гришина Н.В. Организация комплексной системы защиты информации. – М.: Гелиос АРВ, 2007. – 256 с.

ii. Основы информационной безопасности. Учебное пособие для вузов /Е.Б.Белов, В.П.Лось, Р.В.Мещеряков, А.А.Шелупанов. – М.: Горячая линия – Телеком, 2006. – 544 с.

iii. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. – СПб.: Наука и техника, 2004. – 384 с.

iv. Соколов А.В., Степанюк О.М. Защита от компьютерного терроризма. Справочное пособие. – СПб.: БХВ-Петербург – Арлит, 2002. – 496 с.

v. Леонтьев В.П. Безопасность в сети Интернет. – М.: ОЛМА Медиа Групп, 2008. – 256 с.

vi. Гульев И.А. Компьютерные вирусы, взгляд изнутри. – М.: ДМК, 1998. – 304 с.

vii. Защита компьютерной информации/ Терехов А.В., Чернышов В.Н., Селезнев А.В., Рак И.П. – Тамбов: Изд-во ТГТУ, 2003. – 49 с.

viii. ACM Code of Ethics and Professional Conduct// Association for Computing Machinery. –[Електронний ресурс]. – http://www.acm.org/about/code-of-ethics. Заголовок з екрану. Мова англ., дата публікації: 16.10.1992 р.

ix. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях/ Под ред. В.Ф.Шаньгина. – 2-е изд., перераб. И доп. – М.: Радио и связь, 2001. – 376 с.

x. Щербаков Л.Ю., Домашев А.В. Прикладная криптография. Использование и синтез криптографических интерфейсов. – М.: Русская редакция, 2003. – 416 с.

xi. Скоромников К.С. Компьютерное право Российской Федерации: Учебник. – М.: Изд-во МНЭПУ, 2000. – 224 с.

xii. Конвенція про кіберзлочинність// Офіційний вісник України. – 2007, № 65. – С. 2535.

xiii. Некрасов Всеволод. Сотрудник – первая угроза информационной безопасности// IT Business Week. – [Електронний ресурс]. – http://pda.itbusiness.com.ua/content/view/5207/38/. Заголовок з екрану. Мова рос., дата публікації: 19.05.2008 р.

xiv. Закон України «Про інформацію» № 2658 XII від 2 жовтня 1992 року// Відомості Верховної Ради України. – 1992, № 48. – С. 650.

xv. Закон України «Про державну таємницю» № 3855-XII від 21 січня 1994 року// Відомості Верховної Ради України. – 1994, № 16. – С. 93.
xvi. Указ Президента України «Про Перелік посадових осіб, на яких покладається виконання функцій державного експерта з питань таємниць» № 452/2006 від 29 травня 2006 року// Офіційний вісник України. – 2006, № 22. – С. 1603.
xvii. Наказ Служби безпеки України «Про затвердження Зводу відомостей, що становлять державну таємницю» № 440 від 12 серпня 2005 року// Офіційний вісник України. – 2005, № 34. – С. 2089.
xviii. Закон України «Про Національну програму інформатизації» № 2684-III від 4 лютого 1998 року// Відомості Верховної Ради України. – 1998, № 27-28. – С. 181.
xix. Закон України «Про електронний цифровий підпис» № 852-IV від 22 травня 2003 року// Відомості Верховної Ради України. – 2003, № 36. – С. 276.
xx. Цивільний кодекс України// Офіційний вісник України. – 2003, № 11. – С. 461.
xxi. Закон України «Про порядок висвітлення діяльності органів державної влади та органів місцевого самоврядування в Україні засобами масової інформації» № 539/97-ВР від 23 вересня 1997 року // Відомості Верховної Ради, 1997. – № 49. – С. 299.
xxii. Закон України «Про ліцензування певних видів господарської діяльності» № 1775-III від 1 червня 2000 року// Відомості Верховної Ради, 2000. – № 36. – С. 299.
xxiii. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» № 80/94-ВР від 5 липня 1994 року// Відомості Верховної Ради, 1994. – № 31. – С. 286.
xxiv. Постанова Кабінету Міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» № 373 від 29 березня 2006 року// Офіційний вісник України, 2006. – № 13. – С. 878.
xxv. Конституція України// Відомості Верховної Ради, 1996. – № 30. – С. 141.
xxvi. Кримінальний кодекс України// Відомості Верховної Ради УРСР, 1961. – № 2. – С. 14.
xxvii. Господарський кодекс України// Відомості Верховної Ради, 2003. – № 11. – С. 462.
xxviii. Закон України «Про телекомунікації» № 1280-IV від 18 листопада 2003 року// Відомості Верховної Ради, 2004. – № 12. – С. 155.
xxix. Закон України «Про Службу безпеки України» № 2229-XII від 25 березня 1992 року// Відомості Верховної Ради, 1992. – № 27. – С. 382.
xxx. Закон України «Про авторське право і суміжні права» № 3792-XII від 23 грудня 1993 року// Відомості Верховної Ради, 1994. – № 13. – С. 64.