Михайло Прокофьєв, Володимир Хорошко*
Національний технічний університет України «КПІ»,
**Національний авіаційний університет*
УДК 004.684.3

ПРОБЛЕМИ ЗАХИСТУ ІНФОРМАЦІЇ В УКРАЇНІ

Анотація: ***На підставі системного і предметного аналізу змісту і раціональних шляхів здійснення функцій захисту сформульовані десять завдань першого виду і чотири класи завдань другого виду. Сформульовано, проаналізовано та описано комплекс проблем, які умовно розбиті на: правові, нормативно-методичні, технічні, організаційні, метрології та технічного регламенту.***
Abstract: ***In the article on the basis of systematic and objective analysis of the content and efficient ways to implement the functions of information security formulated ten tasks of the first type and four class of the second type. Formulated, analyzed and described the complex issues that conditionally divided into: legal, regulatory, methodical, technical, organizational, metrology and technical regulations.***
Ключові слова: ***Захист інформації, система технічного захисту інформації.***

I Вступ

Одне з найбільш фундаментальних положень системно-концептуального підходу до захисту інформації (ЗІ) полягає в тому, що для регулярного та надійного її захисту необхідна повна і несуперечлива концепція захисту [1]. Основною концептуальною вимогою захисту інформації є безліч функцій задач захисту. Основною концептуальною вимогою, яка повинна задовольняти безліч функцій, полягає в системному забезпеченні ЗІ при раціональному використанні асигнувань, що виділяються на захист. Виходячи з розвитку механізмів захисту, мають бути передбачені два види функцій захисту:

- перша функція – створення системно-повних механізмів захисту;
- друга функція – безперервне і оптимальне управління механізмами захисту.

Здійснення функцій ЗІ досягається вирішенням захисту, що включає методи і заходи, здійснювані з метою повного або часткового вирішення однієї або декількох функцій захисту в одній або декількох зонах захисту. У механізмах ЗІ мають бути передбачені задачі для здійснення всіх функцій захисту в усіх зонах захисту для обох видів захисту і всіх дестабілізуючих факторів.

На підставі системного і предметного аналізу змісту і раціональних шляхів здійснення функцій ЗІ сформовано десять [1] завдань першого виду (розв'язуваних з метою створення механізмів захисту) і чотири класи завдань другого виду (розв'язуваних з метою управління механізмами захисту).

Для формування найбільш повного арсеналу потенційно можливих засобів захисту необхідно здійснити системний аналіз можливостей вирішення різних завдань захисту засобами різних класів. Розроблений класифікатор засобів вирішення завдань захисту інформації враховує сутність і зміст класів завдань [2]. Класифікатор містить класи: введення надмірності елементів; резервування елементів системи; регулювання доступу до елементів захисту; регулювання використання елементів системи; маскування інформації; контроль елементів системи; реєстрація відомостей; знищення інформації; сигналізація про атаки та реагування на них. З метою створення найбільш сприятливих умов для розробки і використання перерахованих засобів необхідно провести системний аналіз цих засобів у межах кожного класу.

Тому одним із головних напрямків державної інформаційної політики є створення сучасної системи охорони та захисту інформації. Основною метою функціонування цієї системи є забезпечення безпеки інформації, тобто мінімізації неприпустимого ризику, пов'язаного з можливістю нанесення збитку державі, юридичним особам усіх форм власності та громадянам внаслідок незаконного отримання інформації та її використання.

У сучасних умовах до 86% об'єму втрат інформації пов'язані з несанкціонованим отриманням та її використанням. У першу чергу це стосується технічних каналів витоку інформації. Тому система технічного захисту інформації (СТЗІ) є досить важливою складовою загальної системи забезпечення охорони інформації. СТЗІ призначена для своєчасного виявлення і нейтралізації загроз порушення конфіденційності, цілісності та доступності інформації як з обмеженим доступом (наприклад, «комерційна таємниця», «конфіденційна інформація» та ін.), так і інформації, що становить державний інформаційний ресурс, від витоку технічними каналами.

Для подальшого розвитку СТЗІ в Україні необхідно постійно вирішувати задачі, що стосуються усього комплексу проблем у сфері технічного захисту інформації, серед яких виділяють умовно чотири групи [1]: правові, нормативно-методичні, технічні та організаційні.

II Правові проблеми

Недосконаліть, а по ряду питань відсутність, правової бази істотно ускладнює розгортання діяльності в галузі технічного захисту інформації (ТЗІ). Виходячи з того, що ТЗІ є підсистемою, що входить в загальну систему охорони інформації, вважаємо, що правові проблеми ТЗІ неможливо вирішувати без вирішення правових проблем загального рівня.

У результаті аналізу [3] законодавчої бази України в галузі інформаційних відносин можна виділити наступні основні правові проблеми загальної системи охорони інформації.

По-перше, це відсутність чіткого визначення прав та обов'язків учасників інформаційних відносин, у тому числі щодо питань ЗІ з обмеженим доступом.

По-друге, недостатньо чітка регламентація виникнення права власності на інформацію внаслідок того, що інформація може бути відображена в / на різних носіях і створюватися різними способами. Наразі законодавчо не визначена досить чітко процедура встановлення права власності на інформацію, особливо створену за допомогою технічних засобів, у тому числі засобів обчислювальної техніки.

По-третє, відсутність чіткої деталізації правових норм, що визначають право особистості розпоряджатися інформацією про себе. Як відомо, останнім часом дані про особу накопичуються в різних базах даних, починаючи від бібліотечних і кінчаючи базами даних спецслужб. Обробка даних в таких базах все частіше проводиться за допомогою обчислювальної техніки з використанням хмарних технологій. Тому існує потенційна небезпека безконтрольного або зумисного поширення інформації з цих баз про конкретну особу без її відома, в тому числі і технічними каналами.

По-четверте, потрібно досить чітке визначення виду, типу, обсягу такої інформації з обмеженим доступом як конфіденційна (для службового користування, конфіденційної – комерційної, професійної інформації: лікарської, адвокатської, банківської таємниці тощо); визначення процедури віднесення відомостей до такої інформації і зняття обмежень; визначення прав, обов'язків і відповідальності суб'єктів інформаційних відносин у питаннях визначення категорії такої інформації, її використання та охорони.

Для того, щоб бути достатньо коректним, слід зазначити, що правові проблеми загальної системи охорони інформації, у свою чергу, не можуть бути вирішені без вирішення правових проблем всього комплексу інформаційних відносин.

Тому, на наш погляд, безпосереднє регулювання державними органами має стосуватися тільки тих інформаційних відносин, які пов'язані з інформацією, що становить державну або іншу передбачену законом таємницю, з конфіденційною інформацією, що становить державний інформаційний ресурс, а також з інформацією про особу (персональні дані).

Отже, при розробці законодавчої бази з технічного захисту інформації та у сфері інформаційних відносин повинні бути враховані наступні принципи:

- закони мають бути одними з правових актів, що регулюють правові відносини в інформаційній сфері;
- закони мають бути максимально прямої дії, тобто без посилання на інші нормативні акти, що дозволить їм почати працювати відразу після прийняття;
- закони мають носити в основному регулятивний характер, а не заборонний;
- закони мають носити нормативний характер, тобто визначати права, обов'язки і гарантії суб'єктів правовідносин, що регулюються цими законами.

III Нормативно-методичні проблеми

Закони і підзаконні акти складають верхній ешелон документів, що регламентують правовідносини у галузі технічного захисту інформації. Вони можуть тільки концептуально визначати деякі підходи та особливості технології технічного захисту. Основний же зміст робіт з ТЗІ та оцінювання їх ефективності міститься в спеціальній нормативній документації.

Наявність комплексної, функціонально повної системи документації, що регламентує всі етапи проведення заходів ТЗІ, а також весь життєвий цикл засобів ТЗІ (розробка, виготовлення, випробування, експлуатація, ремонт, зберігання і утилізація) є досить важливим системоутворюючим фактором, що впливає на ефективність функціонування всієї системи ТЗІ в державі.

Тому створення науково обґрунтованої системи нормативних документів є досить актуальним завданням. Хоча наразі є деяка кількість нормативних документів, які відповідають на окремі питання і дають можливість вирішувати деякі завдання за окремими напрямами ТЗІ [1, 3].

Основне рішення цієї проблеми бачиться в створенні системи стандартів та нормативних документів у галузі ТЗІ. В основу класифікації цієї системи може бути покладений матричний принцип.

У цьому випадку основний поділ системи стандартів і нормативних документів буде проводитися за функціональними групами: основоположні стандарти, стандарти та нормативні документи за напрямами і на

продукцію, послуги, процеси і т. і. А всередині цих груп – по предметній області. За основу для предметного поділу слід взяти види технічних розвідок або, що більш обгрунтовано, види і типи носіїв інформації. Створювана система стандартів і нормативних документів одночасно стане нормативною базою для системи сертифікації засобів ТЗІ.

Ще одна досить важлива проблема, яка умовно теж може бути віднесена до нормативної. Перед початком робіт при визначенні переліку необхідних заходів з ТЗІ в кожному конкретному випадку має бути визначений перелік загроз для інформації. Таке визначення можливе лише на основі аналізу моделей загроз і технічних розвідок.

Сучасний підхід до вирішення завдань ТЗІ вимагає створення досконалих моделей, які б описували всі процеси, що відбуваються в системах, і їх загрози. Основна відмінність сучасних моделей полягає в тому, що вони повинні мати динамічний характер, тобто щоб поряд зі статистичними відомостями загального характеру вони дозволяли б здійснювати ситуаційне моделювання процесу ведення розвідки за допомогою конкретних технічних засобів розвідки різного призначення з прив'язкою до конкретного об'єкта розвідки. При цьому з'являється можливість одержання конкретної моделі загроз для кожного конкретного об'єкта, в якому необхідно захистити інформацію з обмеженим доступом на основі використання моделі технічних розвідок і моделі типових загроз [2]. Звичайно, реалізація подібної моделі можлива лише у вигляді комплексу програмно-апаратних засобів на базі ЕОМ з обов'язковим використанням цифрових електронних карт.

Створення такої конкретної моделі та її комплексування з моделлю загроз, яка буде описувати у вигляді математичних моделей реальні технічні канали витоку інформації, технічні засоби захисту і процеси захисту інформації, дозволяє створити замкнену систему моделювання конфліктної боротьби – систем розвідки і захисту. Це дозволить використовувати різні оптимізаційні або експертні методи для підвищення ефективності прийнятих рішень щодо захисту інформації, особливо, якщо це стосується СТЗІ великих об'єктів.

IV Технічні проблеми

Розвиток засобів технічних розвідок (ЗТР) базується на останніх досягненнях науки, техніки і технології. Тому засоби протидії, тобто засоби ТЗІ, повинні створюватися з урахуванням цих обставин. В цілому проблема розробки та виробництва засобів ТЗІ, а також методів і способів ТЗІ, за своїм змістом є досить наукомісткою та багатогранною. Ці обставини визначають необхідність концентрації наукових та інженерних зусиль для вирішення наступних основних проблем [1, 2, 4]:

- дослідження перспектив розвитку та можливостей технічних розвідок в умовах певної невизначеності інформації про них;
- виявлення, дослідження та оцінювання інформативності можливих технічних каналів витоку інформації в умовах їх можливого комплексування;
- розробка і виробництво вітчизняних технічних засобів захисту, захищених засобів обробки інформації та засобів для оцінювання захищеності з урахуванням застосовуваних і розроблюваних технічних засобів розвідки.

Аналіз всього спектра загроз дозволяє зробити висновок про те, що, як правило, найбільш інформативними є технічні канали витоку, пов'язані з мовною інформацією і з інформацією, що циркулює в інформаційно-телекомунікаційних системах і автоматизованих системах управління.

Останнім часом все частіше з'являються повідомлення про використання для несанкціонованого доступу до мовної інформації засобів, принципи роботи яких засновані на застосуванні методів високочастотного нав'язування і оптичного зондування об'єктів (лазерних засобів розвідки) [1]. Необхідно оцінювати інформативність і небезпеку таких каналів витоку інформації. За умови позитивного оцінювання наявності таких каналів витоку на об’єктах інформаційної діяльності слід розробити методи і засоби щодо їх нейтралізації [4].

Особливої гостроти проблема ТЗІ набуває в сучасних умовах, коли засоби обчислювальної техніки і різні інформаційні технології інтенсивно впроваджуються в усі галузі людської діяльності. Оскільки проблема комп'ютерної безпеки є багатоплановою і багатогранною, то необхідно розгортати роботи з ТЗІ за багатьма напрямками – від розробки теоретичних основ інформаційної безпеки комп'ютерних систем до розробки програмних і апаратних засобів технічного захисту. Особливе місце в цьому ряду займає захист від атак в мережі Інтернет і від програмних закладок. Серед основних проблем, які необхідно вирішувати найближчим часом, слід назвати наступні [2]:

- удосконалення визначення рівнів захищеності інформації;
- розробка критеріїв захищеності інформації;

– розробка функціональних наборів апаратно-програмних засобів, що забезпечують досягнення певного (заданого) рівня захищеності інформації;
– розробка апаратно-програмних засобів захисту інформації;
– розробка методів сертифікації (експертизи) апаратно-програмних засобів захисту інформації;
– розробка методів сертифікації (експертизи) систем захисту інформації на відповідність рівням захищеності;
– розробка спеціальних засобів електронно-обчислювальної техніки (ЕОТ), операційних систем, що забезпечують найвищий рівень захищеності інформації.

Слід враховувати, що вирішення цих проблем може мати специфічні особливості для засобів ЕОТ, автоматизованих (інформаційних) систем, локальних і розподілених мереж.

При розробці технічних засобів ТЗІ і захищених засобів, що призначені для оброблення інформації з обмеженим доступом, наразі необхідно враховувати й інші предметні області та фактори.

V Організаційні проблеми

Серед цілого ряду організаційних проблем необхідно виділити на наш погляд одну, вирішувати яку слід лише за рахунок залучення широкого кола висококваліфікованих фахівців – мова йде про створення системи підготовки, підвищення кваліфікації та перепідготовки фахівців з питань ТЗІ.

Забезпечення режиму захисту інформації в умовах, які постійно змінюються і ускладнюються, неухильно вимагає проведення:
– функціональних і прикладних досліджень явищ і процесів у сфері ТЗІ;
– визначення необхідної кількості підготовлених і компетентних фахівців з ТЗІ.

Наслідком цього процесу і стала поява модифікації і певних тенденцій у системі підготовки, підвищення кваліфікації та перепідготовки фахівців з ТЗІ. Тому саме життя визначає наступні цілі в цій області [5]:
– підготовка, підвищення кваліфікації та перепідготовка фахівців, які вміють ефективно вирішувати виникаючі завдання з ТЗІ в Україні;
– збільшення чисельності фахівців, які проходять підготовку, перепідготовку та підвищення кваліфікації за направленням ТЗІ;
– об'єднання зусиль провідних навчальних і наукових колективів, адміністративних органів для вирішення масштабних практичних завдань з ТЗІ;
– створення та постійний розвиток регіональних наукових шкіл у галузі ТЗІ;
– створення умов для забезпечення режиму інформаційної безпеки держави в цілому, в регіонах, організаціях та окремих громадян.

Згідно зі сформульованими цілями має проводитись розробка методичного забезпечення для навчального процесу та проведення його за наступними напрямками [5]:
– розробка та обґрунтування концепції, підвищення кваліфікації та перепідготовки фахівців із захисту інформації;
– розробка кваліфікаційних та обґрунтованих вимог до фахівців з ТЗІ;
– розробка навчальних планів підготовки, підвищення кваліфікації та перепідготовки фахівців з ТЗІ;
– розробка навчальних програм з дисциплін, визначених навчальними планами;
– розробка навчально-методичних посібників з дисциплін, визначених навчальними планами.

Перший напрямок вочевидь має включати в себе дві частини: аналіз існуючої структури навчання фахівців з ТЗІ та розробку концептуальних положень підготовки, підвищення кваліфікації та перепідготовки фахівців у області ТЗІ.

У першій частині першого напряму необхідно розглядати категорії становлення та розвитку системи навчання кадрів з ТЗІ до сучасного і якісного рівня.

Проведені дослідження [5] підтверджують, що в другій частині першого напряму виділяються чинники, які визначають концепцію навчання фахівців з ТЗІ. До найважливіших чинників належить необхідність:
– підвищення потреби в професійних кадрах з ТЗІ, яка обумовлена різким збільшенням обсягу і складу інформації, що вимагає надійного і заданого рівня її захисту;
– підвищення якості підготовки фахівців у зв'язку з ускладненням умов, в яких здійснюється захист державних секретів, комерційної таємниці і т. і.;
– використання всіх форм навчання (підготовка, підвищення кваліфікації, перепідготовка) для задоволення потреб у фахівцях з ТЗІ;
– використання диференційного підходу до навчання фахівців, який диктується тим, що в сучасних умовах потрібні не тільки фахівці-універсали з комплексного захисту інформації, але і висококваліфіковані фахівці з окремих конкретних напрямків з ТЗІ (організаційно-правових, інженерно-технічних, апаратних, апаратно-програмних, криптографічних) і з урахуванням галузевої специфіки (телекомунікації і зв'язок,

авіаційний зв'язок, системи управління тощо), для підготовки яких необхідно вводити нові спеціальності та напрямки навчання.

VI Проблеми метрології та регламенту в системі ТЗІ

В Україні існує система нормативно-правових і нормативно-технічних актів щодо метрологічного забезпечення єдності вимірювань та простежуваності їх результатів з метою встановлення відповідності заходів в тому числі і з захисту інформації встановленим нормам та правилам (стосується усіх зазначених вище груп проблем захисту інформації). Схематично існуючу систему нормативно-правових і технічних актів можна зобразити як піраміду, верхівку якої займає Конституція України.

Аналіз змісту діючих на сьогодні нормативних документів у сфері ТЗІ свідчить, що з позицій метрології в них не регламентується вживання уніфікованих показників точності результатів вимірювань (випробувань), вони спираються на різні методи їх оцінювання, відображають різні підходи до вирішення вимірювальних завдань і тому погано узгоджуються один з одним. Недостатньо уваги приділено визначенню кваліфікації виконавців робіт у сфері ТЗІ. Все це не сприяє забезпеченню єдиного підходу до проведення випробувань (інструментального контролю та атестації) в системі ТЗІ.

Неузгодженість вимог нормативно-правових актів може привести до недостовірних результатів при проведенні вимірювань значень параметрів ПЕМВН. Відсутність в документації на проведення випробувань умов і характеристик, при яких були визначені декларовані параметри, роблять неможливим коректний перерахунок відповідних величин. У результаті отримуємо некоректні результати вимірювань приладами, призначеними для інших цілей, ніж для вимірювань в області ПЕМВН.

Базовим елементом нормативно-правового регулювання в області ТЗІ має бути технічний регламент як документ, який встановлює обов'язкові для застосування і виконання вимоги до об'єктів технічного регулювання, зокрема мають бути розроблені спеціальні технічні регламенти забезпечення безпеки інформаційних технологій і вимог до засобів забезпечення безпеки інформаційних технологій. Регламент з захисту інформації обмеженого доступу має визначати комплекс організаційних і технічних заходів в частині захисту такої інформації при її обробці, зберіганні і передачі каналами зв'язку.

Для його розробки необхідно визначити: межі дії технічних регламентів; основні поняття в області інформаційних технологій, перелік об'єктів технічного регулювання, для яких ризик реалізації загроз може бути недопустимо великий, види потенційних загроз безпеці інформації і основні способи їх реалізації, порядок аналізу і оцінки ризиків для загроз безпеці інформації, категорії об'єктів технічного регулювання залежно від ризиків реалізації загроз, правила віднесення об'єктів технічного регулювання до встановлених категорій, вимоги безпеки для кожної категорії об'єктів технічного регулювання. Для цього слід системно провести аналіз діючих в Україні нормативно-правових актів, міжнародних і національних стандартів, інших нормативно-методичних документів, що регламентують вимоги безпеки в області інформаційної безпеки, а також проаналізувати досвід їх практичного використання.

При розробці технічних регламентів слід сформувати перелік міжнародних і національних стандартів в сфері ТЗІ, а також інших нормативно-методичних документів, використовуваних для вирішення задач інформаційної безпеки; провести аналіз інформації про інциденти безпеки, що відносяться до наочної області технічних регламентів; визначити і сформулювати особливості набирання чинності технічних регламентів і сформулювати вимоги до перехідного періоду, необхідні форми і схеми підтвердження відповідності залежно від категорій об'єктів технічного регулювання, порядок проведення контролю і нагляду.

VII Висновки

Перераховані фактори обумовлюють концептуальні положення системи забезпечення захисту інформації в Україні та навчання фахівців з ЗІ, які повинні включати мережу навчальних закладів, що забезпечують необхідну якісну підготовку, перепідготовку та підвищення кваліфікації як з комплексного захисту інформації, так і по кожному з напрямків із захисту інформації.

З викладеного очевидно, що для виконання вимог нормативно-правової бази щодо захисту інформації від витоку каналами ПЕМВН слід виконувати і вимоги законодавства з метрології.

У цілому всі названі і багато інших проблем можуть бути вирішені тільки в результаті створення нормально функціонуючої національної системи технічного захисту інформації. Розвиток і становлення такої системи може бути реалізовано тільки шляхом об'єднання зусиль різних міністерств, відомств, організацій, установ, підприємств, а також зусиль провідних вчених, інженерів і практиків.

Список використаної літератури. ***1.*** *Ленков С. В. Методы и средства защиты информации. В 2-х томах /Ленков С. В., Перегудов Д. А., Хорошко В. А.– К.: Арий,2008.* ***2.*** *Емельянов С. Л. Проблемы защиты информации от утечки и пути ее решения / Емельянов С. Л.– Одесса: Фенікс, 2011. – с. 624* ***3.*** *Артемов В. Ю. Нормативно-правовий довідник з охорони інформації в Україні. У 4-х томах / Артемов В. Ю., Лєнков О. С., Пашков А. С., Стаднік О. М., Хорошко В. О. – К.: Вид. ДУІКТ, 2010.* ***4.*** *Бабак В. П. Теоретические основы защиты информации / Бабак В. П., Ключников А. А. – НАН Украины, Ин-т проблем безопасности АЭС.– Чернобыль (Киев.обл.): Ин-т проблем безопасности АЭС, 2012.– с.776* ***5.*** *Хорошко В. О. Методичне забезпечення підготовки та перепідготовки спеціалістів з інформаційної безпеки / Хорошко В. О., Орєхова І. І. // Сучасна спеціальна техніка, №3, 2011. – С. 22-27.*

Дмитро Мехед
Чернігівський національний технологічний університет

УДК 004.773

ІНФОРМАЦІЙНА БЕЗПЕКА В СОЦІАЛЬНИХ МЕРЕЖАХ. МЕТОДИ ПОШИРЕННЯ ІНФОРМАЦІЇ В СОЦІАЛЬНИХ МЕРЕЖАХ

Анотація: **Розглядаються соціальні мережі, основні методи поширення інформації в соціальних мережах, зроблено аналіз переваг і недоліків різних методів захисту інформації. Проаналізовано метод визначення стратегії розповсюдження інформації в соціальній мережі, виділено основні параметри, які є базовими для забезпечення захисту інформації, можливість втрати інформації, а також методи її захисту.**
Summary: **In the article the social networks, the main methods of dissemination of information in social networks, the analysis of the advantages and disadvantages of various methods of data protection. The analysis method for determining the strategy of information dissemination in social networks highlights the main parameters that are fundamental to protect information, the possibility of loss of information, as well as methods of protection.**
Ключові слова: **Інформація, інформаційна безпека, соціальні мережі.**

Характерною особливістю сучасності є та обставина, що до активної участі в інформаційних процесах у дуже стислі строки долучилися широкі маси користувачів, що в переважній більшості не мають відповідного рівня підготовки до участі в суспільно корисній інформаційній діяльності. Для значної частини учасників інформаційних обмінів самовираження в Інтернеті поки що є значущим як процес. І тому сьогодні інформаційний простір перевантажений випадковою, низькоякісною інформацією, що ускладнює використання суспільно значущих ресурсів. Однак останнім часом з розвитком інформаційних технологій, удосконаленням загальносуспільної системи соціальних інформаційних комунікацій в Україні ми спостерігаємо характерний також і для інших країн світу процес самоорганізації вітчизняного інформаційного простору, формування системи соціальних інформаційних мереж [1].

Є два різні способи, за допомогою яких людина отримує інформацію в мережі: – через зв'язки в соціальних мережах і під впливом зовнішніх немережевих джерел, таких як традиційні ЗМІ [2]. Хоча більшість нинішніх моделей сприйняття інформації в мережах виходять з того, що інформація лише передається від одного вузла до іншого по краях (периферії) базової мережі, доступність даних в масових соціальних мережах в Інтернеті дозволяє нам докладніше дослідити цей процес. Таким чином соціальні мережі відіграють фундаментальну роль у поширенні інформації.

Соціальна мережа (від англ. Social networking service) – платформа, онлайн сервіс або веб-сайт, призначені для побудови, відображення та організації соціальних взаємовідносин, візуалізацією яких є соціальні графи [3]. Наразі кількість соціальних мереж в Інтернеті і число їх користувачів швидко зростає (соціальні мережі стартували в 1995 р, в 2000-і набули глобального розмаху).

Соціальні мережі – явище нове, але йому передував ряд філософських концепцій. Наприклад, китайська концепція Guanxi про використання особистого впливу на основі особливого виду особистих відносин, таких як повага, дружнє ставлення та готовність надати один одному взаємну допомогу або послугу [3]. Цю концепцію пов'язують з поняттями «суспільство», в якому індивіди більш орієнтовані на дотримання інтересів оточуючих, ніж своїх власних.

Особиста інформація ще ніколи не була такою доступною, як нині. Ситуація загострюється ще й через те, що більшість користувачів не знає елементарних правил безпеки онлайнового спілкування і використання