УДК 681.322

В.В. Гніліцький, к.т.н., доц.
О.В. Морозов, аспір.
Житомирський інженерно-технологічний інститут

ВИКОРИСТАННЯ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ ЗАХИСТУ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ

В даній роботі викладені підходи щодо створення захищеної комп'ютерної системи на підставі нормативних документів України. Показано можливість використання вітчизняних криптографічних алгоритмів захисту інформації при реалізації такої системи.

Вступ

В сучасному світі комп'ютерні технології ввійшли майже в усі сфери людської життєдіяльності. Електронна інформація, яка циркулює в комп'ютерних системах, визначає дії не тільки великої кількості людей, але і безлічі технічних систем, створених людиною. Отже порушення безпеки при обробці, передачі і збереженні інформації в електронному виді може нанести збитки, ступінь і масштаби яких залежать від важливості інформації і можуть бути співмірні з глобальними катастрофами.

У зв'язку з цим для забезпечення безпеки інформації в сучасних інформаційно-телекомунікаційних системах, які засновані на передових інформаційних технологіях, необхідно застосовувати комп'ютерні системи, які здатні забезпечити захист інформації, що обробляється, від певних загроз і таким чином реалізовувати певну політику безпеки, тобто захищені комп'ютерні системи. При побудові захищених комп'ютерних систем широко застосовуються криптографічні методи, які є базовими для забезпечення надійної ідентифікації та аутентифікації сторін інформаційного обміну, для захисту інформації при передачі по каналах зв'язку тощо.

Сучасний підхід до захисту інформації у комп'ютерних системах на підставі нормативних документів України

В Україні основним нормативним документом, що встановлює основи регулювання правових відносин щодо захисту інформації у комп'ютерній системі, є Закон України "Про захист інформації в автоматизованих системах". Даний документ визначає об'єкти захисту, суб'єкти правових відносин, які пов'язані з обробкою інформації в автоматизованій системі, а також встановлює основні принципи захисту інформації.

На сьогоднішній день стан проблеми захисту інформації у комп'ютерних системах і підходи до її вирішення відображені в нормативних документах системи технічного захисту інформації (НД ТЗІ) [3–7]. Ці документи визначають концепцію вирішення задачі захисту інформації у комп'ютерній системі і дозволяють здійснювати наступне:

- визначати вимоги щодо захисту інформації у комп'ютерних системах;
- створювати захищені комп'ютерні системи та комплекси засобів захисту;
- оцінювати захищеність інформації у комп'ютерних системах і визначити їхню придатність для обробки інформації, яка вимагає захисту.

Розглянемо основні положення НД ТЗІ, що будуть використовуватись надалі.

Згідно з [3] загрози для оброблюваної в автоматизованій системі інформації залежать від характеристик комп'ютерної системи, фізичного середовища, персоналу, а також самої інформації. В даний час існує досить велика кількість різноманітних способів класифікації потенційних загроз, однак найбільш зручним для аналізу є спосіб класифікації загроз за результатом їхнього впливу на інформацію. Загрози можуть впливати на інформацію безпосередньо або опосередковано. Безпосередній вплив на інформацію відбувається за допомогою впливу загрози на властивості інформації, а саме на конфіденційність, цілісність і доступність. Опосередкований вплив на інформацію відбувається за допомогою впливу загрози на властивості комп'ютерної системи, у якій вона обробляється, а саме на керованість і спостережність комп'ютерної системи. При цьому втрата керованості комп'ютерної системи може призвести до її неспроможності захистити оброблювану інформацію, а отже, і до порушення властивостей даної інформації. Втрата спостережності комп'ютерної системи може

призвести до помилкової реєстрації системних подій (порушення процедур автентифікації та ідентифікації, помилкових записів у системному журналі тощо), що також може вплинути на властивості оброблюваної у комп'ютерній системі інформації. Таким чином уся безліч можливих загроз може бути розділена на чотири основні типи:

- загрози конфіденційності – загрози, що відносяться до несанкціонованого ознайомлення з інформацією;
- загрози цілісності – загрози, що відносяться до несанкціонованої модифікації інформації;
- загрози доступності – загрози, що відносяться до порушення можливості використання комп'ютерних систем або оброблюваної інформації;
- загрози керованості і спостережності – загрози, що відносяться до можливості порушення керованості комп'ютерною системою та втрати спостережності за системними подіями, що відбуваються в комп'ютерній системі.

В [6] комп'ютерна система, незалежно від її апаратного та програмного забезпечення, розглядається як перелік деяких функціональних послуг (рис. 1). Кожна послуга являє собою набір функцій, що дозволяють протистояти визначеній множині загроз. Кожна послуга може включати кілька рівнів. Чим вище рівень послуги, тим більш повно забезпечується захист від визначеного виду загроз.

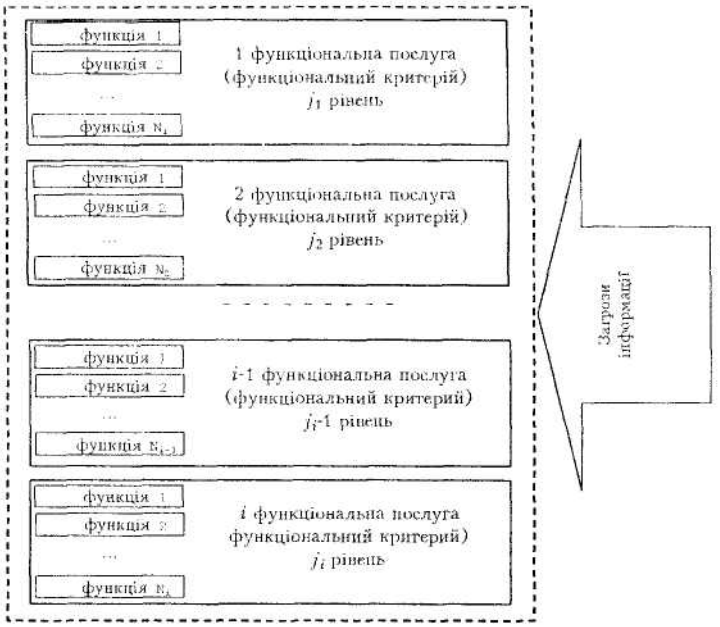

Рис. 1. Комп'ютерна система як перелік функціональних послуг

Базовим поняттям для вирішення задачі захисту інформації у комп'ютерній системі є критерій оцінки захищеності. Кожна функціональна послуга визначається своїм критерієм, що дозволяє визначити необхідні (базові) функції захисту при розробці комп'ютерної системи і створює порівняльну шкалу для оцінки функцій захисту. Функціональні критерії розподілені на чотири групи, кожна з яких описує вимоги до послуг, що забезпечують захист інформації від одного з чотирьох типів загроз:

- критерії конфіденційності;
- критерії цілісності;
- критерії доступності;
- критерії спостережності.

В [7] за сукупністю характеристик автоматизованої системи (конфігурація апаратних засобів обчислювальної системи та їх фізичне розміщення, кількість різних категорій оброблюваної інформації, кількість користувачів і категорій користувачів) виділено три ієрархічні класи автоматизованих систем, вимоги до функціонального складу комплексу засобів захисту яких істотно відрізняються:

• "Клас 1" – одномашинний, однокористувацький комплекс, що обробляє інформацію однієї чи декількох категорій конфіденційності, наприклад, автономний персональний комп'ютер, доступ до якого контролюється з використанням організаційних заходів.

• "Клас 2" – локалізований багатомашинний багатокористувацький комплекс, що обробляє інформацію різних категорій конфіденційності, наприклад, локальна комп'ютерна мережа.

• "Клас 3" – розподілений багатомашинний багатокористувацький комплекс, що обробляє інформацію різних категорій конфіденційності, наприклад, глобальна мережа.

У межах кожного класу автоматизованої системи виділяються підкласи автоматизованих систем, у кожному з яких підвищуються вимоги до забезпечення певних властивостей інформації, а саме конфіденційності, цілісності та доступності. Для кожного з таких підкласів кожного класу вводиться деяка кількість ієрархічних стандартних функціональних профілів захищеності, що являють собою перелік мінімально необхідних рівнів функціональних послуг (функціональних критеріїв), які повинні реалізувати комплекс засобів захисту обчислювальної системи для того, щоб задовольнити вимоги до захищеності інформації, що обробляється в даній автоматизованій системі (рис. 2).

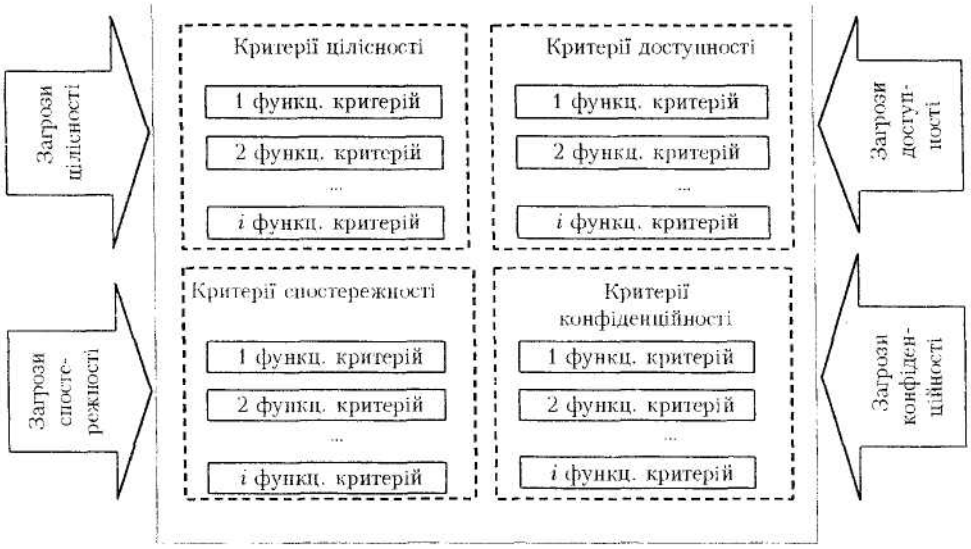

Рис. 2. Стандартний функціональний профіль захищеності автоматизованої системи

Стандартні функціональні профілі захищеності реалізовані на підставі відомих на сьогоднішній день функціональних послуг (функціональних критеріїв) і дозволяють забезпечувати виконання вимог до захисту інформації від множини можливих загроз.

Вибір стандартного функціонального профілю захищеності для реальної комп'ютерної системи

Використовуючи вищевикладений матеріал, розглянемо задачу створення захищеної комп'ютерної системи для забезпечення безпеки інформації, що обробляється на персональному комп'ютері, підключеному до відкритої комп'ютерної мережі, наприклад, глобальної комп'ютерної мережі Інтернет. Для цього необхідно, грунтуючись на стандартному функціональному профілі захищеності, вибрати оптимальну кількість необхідних функцій захисту, що будуть реалізовані комплексом засобів захисту в реальній комп'ютерній системі і забезпечать безпеку оброблюваної у ній інформації.

Відповідно до наведеної вище класифікації автоматизованих систем для персонального комп'ютера, підключеного до відкритої комп'ютерної мережі, найбільш близьким є "клас 3" автоматизованих систем і підклас обраного класу, в якому підвищені вимоги до забезпечення конфіденційності, цілісності та доступності інформації, яка буде оброблятися на визначеному об'єкті обчислювальної техніки.

Згідно з [7] мінімальний стандартний функціональний профіль захищеності для комп'ютерної системи, що входить до складу автоматизованої системи "класу 3", з підвищеними

вимогами до забезпечення конфіденційності, цілісності та доступності оброблюваної інформації, має наступний вид:

КД – 2. Базова довірча конфіденційність;
КО – 1. Повторне використання об'єктів;
КВ – 1. Мінімальна конфіденційність при обміні;
ЦД – 1. Мінімальна довірча цілісність;
ЦО – 1. Обмежений відкат;
ЦВ – 1. Мінімальна цілісність при обміні;
ДР – 1. Квоти;
ДВ – 1. Ручне відновлення;
НР – 2. Захищений журнал;
НИ – 2. Одиночна ідентифікація і автентифікація;
НК – 1. Однонаправлений достовірний канал;
НО – 2. Розподіл обов'язків адміністраторів;
НЦ – 2. Комплекс засобів захисту з гарантованою цілісністю;
НТ – 2. Самотестування при старті;
НВ – 1. Автентифікація вузла.

В даному стандартному функціональному профілі перераховані символьні позначення та повні назви функціональних послуг із вказівкою, у цифровому позначенні, рівня реалізації кожної з послуг. У [6] описані функції захисту кожної з послуг для обраного стандартного функціонального профілю захищеності комп'ютерної системи.

Обраний стандартний функціональний профіль захищеності зручний для проведення аналізу, оскільки має загальний характер і підходить не тільки для окремого комп'ютера, підключеного до відкритої комп'ютерної мережі, а також і для інших обчислювальних систем, наприклад, для корпоративної локальної комп'ютерної мережі з виходом на глобальну комп'ютерну мережу, для розподіленої корпоративної комп'ютерної мережі тощо. Такий підхід дозволить розглядати задачу в загальному виді, незалежно від апаратного забезпечення обчислювальної системи, яка потребує захисту, і полегшить практичну реалізацію для будь-якої реальної комп'ютерної системи.

Вибір криптографічних алгоритмів захисту інформації для реалізації функціональних послуг захищеної комп'ютерної системи

Аналіз опису функцій захисту обраного стандартного функціонального профілю захищеності згідно з [6] дозволяє виділити перелік функціональних послуг, при практичній реалізації яких необхідно використовувати криптографічні алгоритми захисту інформації. На рис. 3 зображені обрані функціональні послуги захищеної комп'ютерної системи з урахуванням взаємозв'язку між ними, які можна умовно розподілити на дві групи:

- функціональні послуги комп'ютерної системи при роботі в автономному режимі;
- функціональні послуги комп'ютерної системи при роботі у відкритій комп'ютерній мережі.

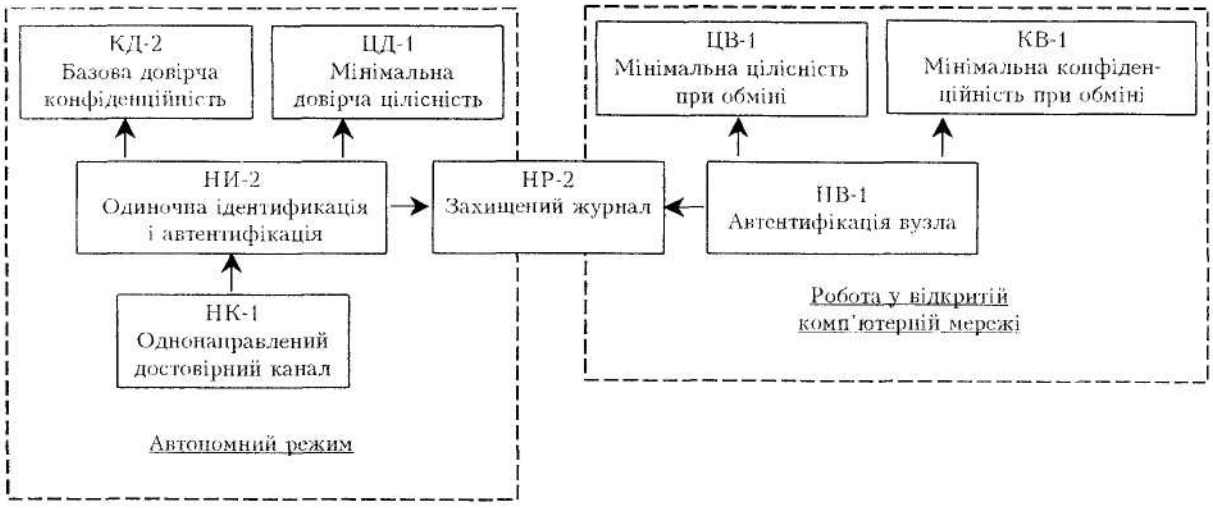

Рис. 3. Функціональні послуги захищеної комп'ютерної системи, які реалізуються з використанням криптографічних алгоритмів

Перша група функціональних послуг захищеної комп'ютерної системи є базовою групою, оскільки функціональні послуги саме цієї групи визначають можливість початкового завантаження захищеної комп'ютерної системи, а також варіанти початкового завантаження і режими функціонування комп'ютерної системи в залежності від встановлених прав доступу користувачів до об'єктів захищеної комп'ютерної системи (режим адміністратора чи режим користувача). Використання криптографічних алгоритмів захисту інформації для реалізації функціональних послуг цієї групи дозволить реалізувати захищений механізм завантаження комп'ютерної системи і забезпечити безпеку інформації під час її обробки і збереження.

Функціональні послуги другої групи визначають режим роботи захищеної комп'ютерної системи при роботі персонального комп'ютера у відкритій комп'ютерній мережі. Функціональні послуги другої групи є необов'язковими при роботі персонального комп'ютера в автономному режимі. Використання даних функціональних послуг можливо тільки після вдалого виконання початкового завантаження захищеної комп'ютерної системи і настройки режиму функціонування комп'ютерної системи. Застосування криптографічних алгоритмів захисту інформації для реалізації функціональних послуг даної групи дозволить виключити можливість несанкціонованого зовнішнього підключення до комп'ютера з боку відкритої мережі.

Окремо від двох груп на рис. 3 виділена функціональна послуга захищеної комп'ютерної системи "НР-2. Захищений журнал", що функціонує на всіх етапах роботи комп'ютерної системи (початкове завантаження, автономна робота, робота в мережі, припинення роботи) і забезпечує реєстрацію всіх системних подій, що мають відношення до безпеки. Використання криптографічних алгоритмів захисту інформації для реалізації даної функціональної послуги викликано вимогами до забезпечення схоронності інформації, що зберігається в "захищеному" журналі.

Аналіз вимог до функціональних послуг захищеної комп'ютерної системи, які зображені на рис. 3, дозволяє попередньо обрати криптографічні алгоритми, що будуть використовуватися для реалізації цих функціональних послуг і підібрати нормативні документи України, що регламентують практичну реалізацію обраних криптографічних алгоритмів. Результати відповідного аналізу і вибору наведені в таблиці 1.

Таблиця 1

Назва функціональної послуги	Розділ криптографії, назва криптографічного алгоритму	Нормативний документ
НК-1. Однонаправлений достовірний канал	Симетрична криптографія, накладання гами	ГОСТ 28147-89
НИ-2. Одиночна ідентифікація і автентифікація	Несиметрична криптографія, алгоритм обчислення хеш-функції	ГОСТ 34.311-95
КД-2. Базова довірча конфіденційність	Симетрична криптографія	ГОСТ 28147-89
ЦД-1. Мінімальна довірча цілісність	Симетрична криптографія	ГОСТ 28147-89
НР-2. Захищений журнал	Симетрична та несиметрична криптографія, алгоритми блокового та потокового шифрування, алгоритм обчислення хеш-функції	ГОСТ 28147-89 ГОСТ 34.311-95
ІВ-1. Автентифікація вузла	Несиметрична криптографія, алгоритм обчислення хеш-функції	ГОСТ 34.311-95
КВ-1. Мінімальна конфіденційність при обміні	Симетрична криптографія, алгоритм потокового шифрування	ГОСТ 28147-89
ЦВ-1. Мінімальна цілісність при обміні	Несиметрична криптографія, алгоритм електронного підпису	ГОСТ 34.310-95

Подальша конкретизація задачі і розробка алгоритмів практичної реалізації функцій захисту для кожної функціональної послуги захищеної комп'ютерної системи, з урахуванням обраних алгоритмів криптографічного захисту інформації, можлива тільки після вибору апаратно-програмної платформи і необхідних засобів розробки.

ЛІТЕРАТУРА:

1. Закон України "Про інформацію", № 2657-XII від 02.10.92 р.
2. Закон України "Про захист інформації в автоматизованих системах", № 80/94-ВР від 05.07.94 р.
3. Нормативний документ системи ТЗІ (НД ТЗІ 1.1-002-99) "Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу", затв. наказом ДСТСЗІ СБ України від 28.04.99 р. № 22.
4. Нормативний документ системи ТЗІ (НД ТЗІ 1.1-003-99) "Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу", затв. наказом ДСТСЗІ СБ України від 28.04.99 р. № 22.
5. Нормативний документ системи ТЗІ (НД ТЗІ 3.7-001-99) "Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі", затв. наказом ДСТСЗІ СБ України від 28.04.99 р. № 22.
6. Нормативний документ системи ТЗІ (НД ТЗІ 2.5-004-99) "Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу", затв. наказом ДСТСЗІ СБ України від 28.04.99 р. № 22 (наказом ДСТСЗІ СБ України від 25.12.2000 р. № 64. Термін дії документа продовжено на невизначений термін).
7. Нормативний документ системи ТЗІ (НД ТЗІ 2.5-005-99) "Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу", затв. наказом ДСТСЗІ СБ України від 28.04.99 р. № 22.
8. ГОСТ 28147-89. Система обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.
9. ГОСТ 34.310-95. Информационная технология. Криптографическая защита информации. Процедура выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма.
10. ГОСТ 34.311-95. Информационная технология. Криптографическая защита информации. Функция хэширования.

ГНІЛІЦЬКИЙ Віталій Васильович – кандидат технічних наук, доцент, завідувач кафедри автоматики і управління в технічних системах Житомирського інженерно-технологічного інституту.

Наукові інтереси:
- цифрова обробка сигналів;
- інформаційні технології.

МОРОЗОВ Олег Володимирович – аспірант Житомирського інженерно-технологічного інституту.

Наукові інтереси:
- захист інформації.

Подано 21.12.2002