УДК 004.056

Грищенко О.В., Резніченко В.А.
Кіровоградський національний технічний університет

Забезпечення захисту комп'ютерних систем та мереж

Широке застосування комп'ютерних технологій у автоматизованих системах обробки інформації і управління призвело до загострення проблеми захисту, що циркулювала у комп'ютерних системах, від несанкційованого доступу. Захист інформацією комп'ютерних системах має низку специфічних особливостей, пов'язані з тим, що перестав бути жорстко що з носієм, може легко і швидко копіюватись і передаватися каналами телефонного зв'язку. Відомо дуже великий число загроз інформації, які можна реалізовані як з боку зовнішніх порушників, і із боку внутрішніх порушників.

Радикальне розв'язання проблеми захисту електронну інформацію то, можливо отримано лише з базі використання криптографічних методів, що дозволяють вирішувати найважливіші проблеми захищеної автоматизованої обробітку ґрунту і передачі. У цьому сучасні швидкісні методи криптографічного перетворення дозволяють зберегти вихідну продуктивність автоматизованих систем. Криптографічні перетворення даних є найефективнішим засобом забезпечення конфіденційності даних, їх цілісності і дійсності. Тільки їх використання у поєднанні з необхідними технічними і організаційними заходами можуть забезпечити захисту від широкого спектра потенційних загроз.

Однією із поважних особливостей масового використання інформаційних технологій і те, що з розв'язання проблеми захисту державного інформаційного ресурсу необхідно розосередження заходів щодо захисту даних серед масових користувачів. Інформація повинна бути захищеною насамперед там, де створюється, збирається, переробляється і тих організаціями, яких зазнають безпосередній шкоди при несанкційованому доступі до даних. Цей принцип раціональний і ефективний: захист інтересів окремих організацій – це складова реалізації захисту держави загалом.

Проблеми, виникаючи з безпекою передачі під час роботи в комп'ютерних мережах, можна розділити втричі основних типи: перехоплення інформації – цілісність інформації зберігається, та її конфіденційність порушена; модифікація інформації – вихідне повідомлення змінюється або повністю підміняється іншим державам і відсилається адресата; підміна авторства інформації. З виникненням загроз з'явилися засоби захисту, які покликані розв'язати проблеми безпеки під час роботи в мережі: криптографія, електронна підпис, аутентифікація, захист мереж.

Після того, як сучасні інформаційні технологій отримали масове застосування, захист інформації зайняв важливу роль у життя сучасної людини. На кожному кроці можна зустріти різноманітні засоби захисту. Але найважливішу нішу займає криптографія. На криптографічних методах ґрунтується застосування електронних платежів, можливість передачі секретної інформації з відкритим мереж зв'язку, і навіть рішення значної частини інші завдання захисту в комп'ютерних системах та інформаційних мережах. Потреби захисту інформації сприяли необхідності масового застосування криптографічних методів, отже до потреби розширення відкритих досліджень, і розробок на цій галузі. Володіння основами криптографії стає важливим для науковців світу й інженерів, які спеціалізуються у сфері розробки сучасних засобів захисту.

Однією з актуальних проблем сучасної прикладної криптографії є розробка швидкісних програмних шифрів блокового типу і навіть швидкісних пристроїв шифрування.

Список використаних джерел

1. *Острейковский В.А. Інформатика: Учеб. посібник для студ. середовищ. проф. навч. закладів. – М.:Висш. шк., 2001. –319с.*
2. *Економічна інформатика / під ред. П.В. Конюховского і Д.Н. Колесова. – СПб.: Пітер, 2000. –560с.*
3. *Інформатика: Базовий курс / С.В.Симонович та інших. – СПб.: Пітер, 2002. –640с.*
4. *Молдовян А.А.,Молдовян Н.А., Рад Б.Я. Криптография. – СПб.: Лань, 2001. – 224с.*