

ЗАХИСТ ІНФОРМАЦІЇ В АВТОМАТИЗОВАНИХ СИСТЕМАХ

В інформаційно-телекомунікаційних системах поняття безпеки є досить широким. Під цим поняттям розуміють надійність роботи комп'ютера, збереження цінних даних, захист інформації від внесення до неї змін не уповноваженими особами, збереження таємниці листування в електронному зв'язку. Зрозуміло, у всіх цивілізованих країнах на варті безпеки громадян стоять закони, але у сфері обчислювальної техніки правозастосовна практика поки розвинена недостатньо, а законодавчий процес не встигає за розвитком комп'ютерних систем, багато в чому спирається на заходи самозахисту.

Завжди існує проблема вибору між необхідним рівнем захисту та ефективністю роботи в мережі. У деяких випадках користувачами або споживачами заходи щодо забезпечення безпеки можуть бути розцінені як заходи з обмеження доступу та ефективності. Однак такі засоби, як, наприклад, криптографія, дозволяють значно посилити ступінь захисту, не обмежуючи доступ користувачів до даних.

Слідом за масовим застосуванням сучасних інформаційних технологій криптографія вторгається в життя сучасної людини. На криптографічних методах засноване застосування електронних платежів, можливості передачі секретної інформації по відкритих мережах зв'язку, а також вирішення великого числа інших завдань захисту інформації в комп'ютерних системах та інформаційних мережах.

Потреби практики призвели до необхідності масового застосування криптографічних методів. Одним з яких є метод мережі Фейстеля (конструкція Фейстеля) – один з методів побудови блокових шифрів. Мережа являє собою певну багаторазову структуру, що повторюється (ітерована) і називається осередком Фейстеля. При переході від однієї комірки до іншої змінюється ключ, причому вибір ключа залежить від конкретного алгоритму. Операції шифрування та розшифрування на кожному етапі дуже прості, і при певній доробці збігаються, вимагаючи тільки зворотного порядку використання ключів. Шифрування за допомогою даної конструкції легко реалізується як на програмному рівні, так і на апаратному, що забезпечує широкі можливості застосування. Більшість сучасних блокових шифрів використовують мережу Фейстеля в якості основи.

Отже необхідність розширення відкритих досліджень та розробок у цій області беззаперечна. Володіння основами криптографії стає важливим для вчених і інженерів, що спеціалізуються в області розробки сучасних засобів захисту інформації, а також в областях експлуатації та проектування інформаційних та телекомунікаційних систем.

Науковий керівник – к.т.н., с.н.с., доц. Ю.І. Хлапонін