УДК 681.3.06

Петро Сергійович Клімушин,
кандидат технічних наук, доцент, доцент кафедри інформаційних технологій та кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ

Андрій Володимирович Білобров,
курсант 3 курсу факультету № 4 Харківського національного університету внутрішніх справ

Криптологія як провідний метод захисту інформації в сучасному суспільстві

У сучасних умовах захист інформації стає все більш актуальною і одночасно все більш складною проблемою. Це обумовлено як масовим застосуванням методів автоматизованої обробки даних, так і широким поширенням методів і засобів несанкціонованого доступу до інформації. Тому особливу роль в організації протидії потенційним загрозам займає підхід, при якому засоби захисту інформації використовуються комплексно, кожне у відповідності зі своїм призначенням. На сьогоднішній день існує багато алгоритмів шифрування, серед яких зустрічаються достатньо вдалі та широко використовувані, що розроблені не тільки спецслужбами, а й приватними особами.

Криптологія розділ науки, що вивчає методи шифрування і дешифрування інформації. Вона включає в себе два розділи: криптографію та криптоаналіз.

Криптографія займається розробкою методів шифрування даних, у той час як криптоаналіз займається оцінкою сильних і слабких сторін методів шифрування, а також розробкою методів, які дозволяють зламувати криптосистеми.

Шифруванням називається процес застосування шифру до повідомлення, що має бути захищеним. До основних характеристик сучасних методів шифрування можна віднести: довжину ключа, складність алгоритму перетворення даних, розмір даних, що обробляються, та ін.

Провідна роль у забезпеченні інформаційної безпеки в інформаційно-телекомунікаційних системах відводиться криптографії. До

© Клімушин П.С., Білобров А.В., 2019

найважливіших завдань, що вирішуються криптографією, відноситься забезпечення:

- конфіденційності відомостей, надаючи доступ до них лише з використанням спеціального ключа;

- цілісності інформації, що гарантує відсутність спотворень (видалення, заміни, модифікування) при передачі;

- автентифікації, перевіркою достовірності відправників і переданої інформації. Одним з найбільш поширених варіантів даної дії вважається доказ з нульовим дозволом, коли відправник підтверджує права, не надаючи одержувачу можливості використовувати отриману інформацію як особисту;

- ідентифікації, шляхом підтвердження суб'єктом, що передає відомості, своєї особистості. Доказ з нульовим розголошенням передбачає підтвердження особистих прав, без права розголосу одержувачем;

- нездійсненності відмови від авторства, для підтвердження обов'язків суб'єкта. Контракт, підписаний суб'єктами і підтверджений електронним підписом, має ті ж передбачені законодавством гарантії, що і підписаний звичайним способом.

Цілісність інформації та автентичність сторін досягається використанням хеш-функції та технології електронного підпису. Конфіденційність інформації забезпечується симетричним та асиметричним методами шифрування.

Методи симетричного шифрування – це метод, за яким ключі шифрування і розшифрування є або однаковими, або легко обчислюються один з одного, забезпечуючи спільний ключ, який є таємним.

Методи асиметричного шифрування – криптографічні алгоритми, в яких використовують пару ключів для кожного учасника протоколу – відкритий для шифрування і таємний для розшифрування, який не може бути обчислений з відкритого ключа за визначений час.

Для сучасної криптографії характерне використання відкритих алгоритмів шифрування, що припускають використання обчислювальних засобів. На сьогодні відомо більше десятка перевірених методів шифрування, які при використанні ключа достатньої довжини і коректної реалізації алгоритму, роблять шифрований текст недоступним для криптоаналізу.

Виділяють такі загальні вимоги для криптографічних методів захисту інформації: зашифроване повідомлення повинно піддаватися читанню тільки при наявності ключа; число операцій, необхідних для визначення використаного ключа шифрування по фрагменту повідомлення і відповідного йому відкритого тексту, повинно бути не менше загального числа можливих ключів; число операцій, необхідних для розшифрування інформації шляхом перебору можливих ключів повинно мати строгу нижню оцінку і виходити за межі можливостей сучасних комп'ютерів; знання алгоритму шифрування не повинно впливати на надійність захисту; незначна зміна ключа повинна призводити до значної зміни виду зашифрованого повідомлення навіть при використанні одного і того ж ключа; алгоритм має допускати як програмну, так і апаратну реалізацію, при цьому зміна довжини ключа не повинна призводити до якісного погіршення алгоритму шифрування.

В останні роки значний інтерес викликає квантова криптографія, вагоме місце в якій займає квантовий розподіл ключів. Квантова криптографія – метод захисту комунікацій, заснований на принципах квантової фізики. На відміну від традиційної криптографії, яка використовує математичні методи, щоб забезпечити секретність інформації, квантова криптографія зосереджена на фізиці, розглядаючи випадки, коли інформація переноситься за допомогою об'єктів квантової механіки. Процес відправки та прийому інформації завжди виконується фізичними засобами, наприклад, за допомогою електронів в електричному струмі, або фотонів у лініях волоконно-оптичного зв'язку.

Технологія квантової криптографії ґрунтується на принциповій невизначеності поведінки квантової системи – неможливо одночасно отримати координати і імпульс частинки, неможливо виміряти один параметр фотона, не спотворивши інший.

У результаті проведеного аналізу джерел з розглянутої проблеми виділені та розглянуті сучасні найбільш поширені методи криптографічного захисту інформації від несанкціонованого доступу. В новітніх інформаційних системах для шифрування повідомлень, які передаються, використовуються симетричні алгоритми шифрування, зважаючи на велику обчислювальну здатність асиметричних алгоритмів, їх застосовують для генерації та поширення сеансових ключів (використовується під час сеансу обміну повідомленнями). Усунути основні недоліки, властиві як симетричним, так і асиметричним методам криптографічного

захисту інформації, дозволяє їх комбіноване використання. Як відомо, у сучасних реальних криптосистемах шифрування даних здійснюється за допомогою «швидких» симетричних блокових алгоритмів, а завданням «повільних» асиметричних алгоритмів стає шифрування ключа сеансу. В цьому випадку зберігаються переваги високої секретності (асиметричні) та швидкості роботи (симетричні).

Таким чином, можна зробити висновок, що криптологія є незамінним фактором підтримання інформаційної безпеки як конкретної особи так і держави в цілому.

Одержано 01.11.2019