Криптографічний захист інформаційних технологій та кібербезпека

М.М. Савчук
КПІ ім. Ігоря Сікорського
м. Київ, Україна
mikhail.savchuk@gmail.com

Вступ

Володіння інформацією і в минулому і нині давало можливість досягти швидкого розвитку і успіху у різних галузях як у глобальному масштабі, так і в конкретних справах. Сьогодні світ переживає період, коли накопичено колосальний об'єм знань, що дозволяє перейти до здійснення справді революційних технологічних рішень.

Сьогодні велика кількість конфіденційної інформації передається в електронному вигляді, на електронних носіях, між ЕОМ звичайними лініями зв'язку. Інформація може продаватися та купуватися, мати ціну, що незрівнянно перевищує ціну матеріального носія.

Останніми роками у світі спостерігається перехід суспільства на принципово новий рівень розвитку, що пов'язано зі стрімким зростанням обсягів інформації, істотним збільшенням швидкості її обробки, розширенням можливостей комутацій для миттєвого обміну повідомленнями з метою комунікації, управління, реагування тощо. Проте одночасно з неймовірними перспективами, які відкривають людству новітні інформаційні технології, все більшого масштабу набувають проблеми забезпечення конфіденційності, цілісності, автентичності, доступності та невідстежуваності інформації, неможливості нав'язування та розповсюдження шкідливої інформації.

Розвиток сучасного кіберпростору нерозривно пов'язаний з появою нових загроз безпеці інформації та інформаційним технологіям. Поширення новітніх ІТ-технологій, зокрема інтернету речей, криптовалют, криптобірж, систем електронних виборів, «розумних контрактів» тощо, кардинально змінює кіберпростір. При цьому зростає кількість кібератак на глобальні критичні інфраструктури: системи електропостачання, керування банківськими та комерційними структурами, транспортом, зокрема аеропортами, глобальні бази даних.

У системах захисту інформаційних технологій істотну роль відведено криптографічним механізмам. Криптографічні методи захисту вважаються одними з найбільш надійних та ефективних.

Задачі та аспекти захисту інформації, основні поняття криптографічного захисту інформації

Цілі та головні задачі захисту інформації:

1) Конфіденційність (секретність) інформації;
2) Цілістність інформації;
3) Автентичність інформації;
4) Доступність інформації;
5) Керованість складних систем;
6) Спостережливість.

Методи і напрямки захисту інформації:

1) Юридичні, правові;
2) Нормативно-методичні;
3) Організаційні;
4) Безпосередні (фізичні);
5) Технічні – захист від витоку інформації по технічним каналам електромагнітному, оптичному, акустичному, виброакустическому;
6) Стеганографічні – приховання факту передачі повідомлення;
7) Криптографічні – перетворення інформації за допомогою математичних алгоритмів;
8) Методи квантової криптографії;
9) Захист кіберпростору.

Класифікація криптосистем

1) *Симетрична криптографія і симетричні криптосистеми* (одноключові, с секретним ключем). У відправника і одержувача повідомлення один і той же секретний ключ, вони знаходяться в рівних (симетричних) умовах, можуть як зашифрувати повідомлення так і розшифрувати за допомогою секретного ключа.
   а) *Класична криптографія і класичні шифри* (ручна криптографія).
   б) *Електромеханічні шифрувалні машини* (п.п. XX століття) рис. 1.
   в) *Сучасна симетрична криптографія і симетричні криптосистеми* (з другої половини XX століття).
2) *Асиметрична криптографія і асиметричні криптосистеми* (двохключові, з відкритим ключем) - з 1976 р.

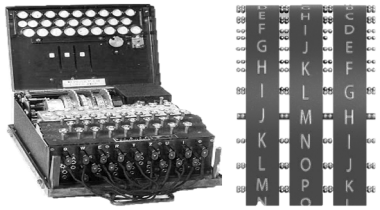

Рис. 1. Приклад електромеханічної шифрувальної машини Другої світової війни Enigma

3) *Квантові криптосистеми. (з 1983 р.)* В таких системах для кодування і передачі інформації використовують стан і квантові властивості елементарних частинок.

Початок криптологічних досліджень у НАН України

Академіки Б.Є. Патон і В.М.Глушков усвідомлювали необхідність розвитку криптологічних досліджень ще на початку 70-х років минулого століття.

В 1973 р. в Інституті кібернетики АН УРСР було створено науково-дослідний підрозділ для проведення криптологічних досліджень під керівництвом тоді члена-кореспондента І. М. Коваленка. До 2019 року академік Ігор Миколайович Коваленко активно працював в різних галузях математики, теоритичної криптології, теорії надійності та масового обслуговування. Він є засновником наукових шкіл в Україні з криптології, теорії надійності, теорії масового обслуговування.

В Інституті кібернетики імені В.М.Глушкова НАНУ розроблено математичний апарат для дослідження дискретних схем, комбінаторно-ймовірнісних алгоритмів, ймовірнісно-алгебраїчних моделей та розв'язання прикладних задач захисту інформаційних технологій. Розроблені методи, алгоритми та отримані результати застосовано для розв'язання актуальних задач у галузі криптографічного захисту інформації.

Факультет інформаційної безпеки Фізико-технічного інституту КПІ ім. Ігоря Сікорського

У 2000 році за ініціативою академіків М.З. Згуровського, І. М. Коваленка створено факультет інформаційної безпеки Фізико-технічного інституту і відкрито три нові кафедри: кафедру математичних методів захисту інформації, кафедру інформаційної безпеки та кафедру фізико-технічних засобів захисту інформації.

Освітня і наукова діяльність кафедр спрямована на підготовку фахівців високо рівня та дослідження в галузі криптографічного, технічного захисту інформації, захисту інформації в комп'ютерних системах, захисту кіберпростору та побудові комплексних систем захисту інформації.

Згідно з рішенням Президії Академії наук України в Києві створено науковий семінар "Проблеми сучасної криптології що з 2001 року активно працює на базі КПІ ім. Ігоря Сікорського, добре відомий фахівцям та активно сприяє розвитку наукових досліджень та підготовці кадрів вищої кваліфікації в сфері захисту інформаційних технологій.

Сучасний стан сфери інформаційної безпеки та кібербезпеки в Україні

Незважаючи на значні досягнення і напрацювання в академічних установах та університетах, необхідно продовжити та посилити дослідження і розробки в галузі криптографічного захисту інформації, стеганографії, кібернетичного захисту.

Існуючі підходи до створення національної системи кібербезпеки не є достаньо ефективними. Стратегія та принципи створення національної системи кібербезпеки потребують перегляду.

Для модернізації і підтримки системи кібербезпеки на належному рівні потрібно постійне проведення інтенсивних наукових досліджень, створення ефективної нормативно-правової бази, залучення професіоналів-практиків.

Проблеми і задачі захисту інформаційних технологій та кібербезпеки

- Фундаментальні проблеми теорії алгоритмів, абстрактної алгебри, теорії чисел.
- Розроблення нових надійних і ефективних систем захисту інформації з врахуванням постійно зростаючих обчислювальних та телекомунікаційних можливостей потенційних порушників систем інформаційної безпеки.
- Розроблення алгоритмів і систем захисту інформації стійких в квантовій моделі обчислень.
- Знаходження нових підходів в вирішенні задач кібербезпеки з використанням теоретичних напрацювань, математичного та статистичного моделювання, машинних обчислень.
- Розроблення математичного, алгоритмічного апарату, програмного забезпечення, технічних засобів для швидкого реагування на постійно виникаючі в системах захисту загрози.
- Розв'язання нових прикладних задач криптографії, стеганографії, криптоаналізу, кібербезпеки.
- Модернізація, покращення нормативно-правової бази для створення ефективної структури захисту інформаційних технологій та кібербезпеки в державі.