7. Співпраця з приватним сектором. Уряд співпрацює з приватним сектором для виявлення та вирішення слабких місць у кіберзахисті та впровадження сучасних технологій захисту.

8. Постійне вдосконалення. Проведення аналізу та оцінки загроз, постійне вдосконалення заходів кібербезпеки з урахуванням сучасних тенденцій у кіберзлочинності та технологій [1].

Ці принципи сприяють забезпеченню ефективного захисту кіберпростору України в умовах протидії збройній агресії та інших кіберзагроз.

Висновок. Таким чином, незважаючи на певні досягнення, виклики в галузі кібербезпеки залишаються значними, і Україна продовжує активно працювати над удосконаленням своїх заходів у цьому напрямку.

Список використаних джерел

1. Закон України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII від 01.01.2024 р.
2. Як забезпечити захист кіберпростору України на тлі збройної агресії рф // [Електронний ресурс] / Режим доступу: https://armyinform.com.ua/2022/09/10/yak-zabezpechyty-zahyst-kiberprostoru-ukrayiny-na-tli-zbrojnoyi-agresiyi-rf/
3. Лєднєй В. Метою діяльності кіберсил ЗСУ є захист суверенітету держави та відсіч збройної агресії в кіберпросторі // [Електронний ресурс] / Режим доступу: https://lb.ua/news/2023/01/31/544318_vadim_liedniey_metoyu_diyalnosti.html

УДК 004.056.5

ПЕРСПЕКТИВИ ЗАСТОСУВАННЯ СУЧАСНИХ КИТАЙСЬКИХ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ

Кацюба В.В., студент, victorkatsiuba2k23@gmail.com, НУ «ЗП»
Козіна Г.Л., к. ф.-м. н., доцент, ainc00@gmail.com, НУ «ЗП»

На сьогодні криптографічний захист інформації є одним із основних складових сучасного захисту інформації. Деякі криптографічні алгоритми через їхню надійність набувають статус національних стандартів, проте існують алгоритми, які ввійшли до міжнародної стандартизації.

Китайські криптографічні алгоритми є одними з них. Їхня простота та надійність, перевірена часом, є головними причинами їхньої поширеності за межами Китаю.

Зокрема технології та протоколи бездротового зв'язку, розроблені в Китаї, використовуються і зараз в мережевій апаратурі.

Це все говорить про потужну позицію Китаю у галузі криптографічного захисту інформації.

Насьогодні використовуються такі чинні китайські стандарти.

1. SM2 – криптографічний алгоритм з відкритим ключем. Використовується в алгоритмах цифрового підпису. Є промисловим стандартом GM/T 0003-2012, національним стандартом GB/T 32918-2017 та міжнародним стандартом ISO/IEC 14888-3:2018.

2. SM3 – алгоритм хешування. У промислову стандартизацію увійшов як GM/T 0004-2012, у національну – як GB/T 32905-2016, у міжнародну - ISO/IEC 10118-3:2018.

3. SM4 – алгоритм блокового шифрування. Промисловий стандарт - GM/T 0002-2012, національний – GB/T 32907-2016, міжнародний – ISO/IEC FDIS 18033-3.

4. Zuc – алгоритм потокового шифрування. Є промисловим GM/T 10004-2012 та міжнародним ISO/IEC 18033-4/Amd.1 стандартом. Також є частиною стандартів 3GPPTM (мобільні телекомунікації) та основою криптографічних алгоритмів 4G-зв'язку EEA3/EIA3 [1, 2].

Сучасні китайські алгоритми засновані на більш перспективних ідеях, які були реалізовані в національних стандартах деяких країн (зокрема, США, Німеччина, Південна Корея, Україна та ін.).

В теперішній час китайські криптоалгоритми успішно імплементуються в Міжнародні стандарти.

Прикладом використання китайських криптографічних алгоритмів є мережевий бездротовий протокол WAPI.

Цей протокол складається з інфраструктури бездротової автентифікації (WAI) для автентифікації особи та бездротової інфраструктури конфіденційності (WPI) для шифрування даних [3].

Шифрування даних в цьому протоколі здійснюється за блоковим алгоритмом SM4 [1].

Протокол WAPI позбавлений вразливостей протоколів WPA2 та WPA3 та використовується більш ніж в 100 операційних системах (включаючи мобільні ОС), більше ніж в 500 моделях інтеграційних схем та більш ніж в 17 тис. моделей промислового, мережевого, IoT- та автообладнання.

На сьогодні Китай має стійку позицію в Міжнародній організації по стандартизації. Він брав участь у 22 підкомітетах SC, на даний момент в ISO внесено 11 патентних декларацій. Також у Китаї є досягнення в області криптографічних алгоритмів нового покоління.

Є наявним вклад у розвиток мережи та зв'язку (наприклад, 5G з використанням алгоритму ZUC), постквантової криптографії (набір алгоритмів PQC та QKD), використання блокчейну в системах електронно-цифрового підпису та захисту конфіденційності.

Також перспективою застосування криптографічних алгоритмів є їхня оптимізація. Існують оптимізації на рівні апаратної архітектури, програмні оптимізації та оптимізації математичного апарату.

Автори більш детально ознайомились з алгоритмом блокового шифрування SM4 [4]. Зокрема вони звернули увагу на можливості оптимізації цього алгоритму з метою покращення його швидкодії. В результаті проведених досліджень та тестування було отримано збільшення швидкодії більш ніж в 2,6 рази.

У подальшому передбачається дослідження потокового шифру ZUC з метою порівняння його з іншими потоковими шифрами, зокрема зі стандартом потокового шифрування України – шифром СТРУМОК.

Висновок. Таким чином, можна побачити, що китайські алгоритми та стандарти є досить ефективними і успішно впроваджуються в міжнародний криптопростір. Автори також продовжують дослідження китайських алгоритмів шифрування та підпису.

Список використаних джерел

1. Huung Z. Chinese Cryptographic Algorithms: Development and Applications. 2020ю
2. Orhanou G., El-Hajji S. The New LTE Cryptographic Algorithms EEA3 and EIA3 Verification, Implementation and Analytical Evaluation. Applied Mathematics & Information Sciences. 2013. Vol. 7, no. 6. P. 2385–2390.
3. Awati R. What is WLAN Authentication and Privacy Infrastructure (WAPI)?. Security. URL: https://www.techtarget.com/searchsecurity/definition/WAPI-WLAN-Authentication-and-Privacy-Infrastructure (date of access: 28.02.2024).
4. Diffie W., George Ledin. SMS4 Encryption Algorithm for Wireless Networks. 2008.