ПРО ІНФОРМАЦІЙНУ БЕЗПЕКУ ГУМАНІТАРНОЇ ІНФОРМАЦІЇ

Журило О. Д., Ляшенко О. С.
Харківський національний університет радіоелектроніки, м. Харків

Наш світ є світом інформації. Передача, накопичення, обробка та зберігання інформації без втрат та пошкоджень стали основою існування підприємств різних форм власності. Інформація стала товаром, який можливо реалізувати, при чому, неодноразово. Крилата фраза, «хто володіє інформацією – той володіє світом», – як неможна краще висвітлює засади існування гуманітарних наук. А як відомо, наявність конкурентоздатного товару часто призводить до появи недобросовісної конкуренції та промислового шпигунства.

Як відомо, основними загрозами безпеці переданої гуманітарної інформації є наступні: несанкціонований доступ до інформації; перехоплення переданих даних зловмисником; аналіз інформації, яка передається; навмисна зміна або пошкодження інформації, що передається; глушіння потоку інформації. Дві останні загрози є такими, які перебувають на найнижчому, фізичному, рівні мережевої моделі. Також на даному рівні можна розглянути таку загрозу, як отримання зловмисником фізичного доступу до джерел інформації.

Найпростішим способом запобігання вказаних небезпек є мікроконтролери. Стартувавши з патенту, отриманого у далекому 1971 р., вони сьогодні стали розповсюдженим засобом керування електронним обладнанням.

Використання у мікроконтролерах досить міцного обчислювального модуля дозволив значно мінімізувати їх габарити, потребу в енергії, та, відповідно, собівартість. Типовим прикладом є мікроконтролери сімейства AVR. Вони дозволяють використовувати для забезпечення безпеки гуманітарної інформації еліптичну криптографію. Найбільш часто вживаними в захищених системах алгоритмами еліптичної криптографії можна назвати: протокол отримання секретного ключа ECDH, алгоритм ECIES, алгоритми для створення цифрового підпису ECDSA та ECSS [1].

Такими алгоритмами можна забезпечити захист інформації. Але такій спосіб, на жаль, не без недоліків. Наприклад, час на виконання криптографічних операцій, досить великий, тому звернення до реальних AVR-мікроконтролерів, що використовують алгоритми еліптичної криптографії, має проводитися не частіше, ніж раз в 30 секунд. У разі застосування софт-реалізацій AVR на основі ПЛІС, що володіють можливістю збільшення максимальної тактової частоти, ЦП більш ніж в 3 рази в порівнянні з оригіналом, даний період часу може бути скорочений к співвідношенню використовуваних частот ЦП [1]. Іншим засобом інформаційного захисту є шифрування, яке дозволяє зберегти в секреті дані, що передаються. Використання вказаних методів допомагає захистити важливу інформацію.

Література:

1. Ляшенко О. С. Моделювання можливих загроз інформаційної безпеки в системах з використанням мікроконтроллерів AVR / О. С. Ляшенко, О. Д. Журило // Перший міжнародний науково-практичний форум «GlobalCyberSecurityForum». Зб. матеріалів форуму. – Харків: ХНУРЕ. 2019. С. 68-70.