УДК 004.056.5
Пархоменко В.В.[1], Зайко Т.А.[2]
[1]студ. гр. КНТ-138 НУ «Запорізька Політехніка»
[2]канд. техн. наук, доц. НУ «Запорізька Політехніка»

АНАЛІЗ ЕФЕКТИВНОСТІ МЕТОДІВ ПІДВИЩЕННЯ СТІЙКОСТІ ЕЛЕКТРОННИХ КЛЮЧІВ ДЛЯ ЗАХИСТУ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Проблеми інформаційної безпеки стали актуальними одночасно з виникненням перших електронно-обчислювальних машин і удосконалювались разом з розвитком технічної бази. Вдосконалення технічної бази систем обробки інформації забезпечило подальший розвиток концепції безпеки, в рамках якої стали виділяти захист технічних засобів, програмного забезпечення і інформації.

Програмне забезпечення – сукупність програм системи обробки інформації і програмних документів, необхідних для експлуатації цих програм.

Безпека програмного забезпечення в широкому змісті є властивістю даного програмного забезпечення функціонувати без прояву різноманітних негативних наслідків для конкретної комп'ютерної системи. Під рівнем безпеки програмного забезпечення (ПЗ) розуміється ймовірність того, що при заданих умовах у процесі його експлуатації буде отриманий функціонально придатний результат.

На сьогоднішній день постали такі проблеми, як незаконне використання алгоритмів, несанкціоноване використання, модифікація, поширення і збут програмних продуктів. Однією з головних проблем є несанкціоноване використання програмного забезпечення. Існують різні типи захисту від несанкціонованого використання, такі як : захист за допомогою компакт-дисків, захист за допомогою електронних ключів, локальний програмний захист, мережевий захист програмного забезпечення, захист програмного забезпечення з прив’язкою до параметрів комп’ютера і активація та інші.

Найпоширенішим захистом програмного забезпечення від несанкціонованого використання є захист за допомогою електронних ключів.

Електронний ключ – це апаратна частина системи захисту, що представляє собою плату з мікросхемами пам'яті і, у деяких випадках, мікропроцесором, поміщену в корпус і призначену для установки в один з стандартних портів ПК (COM, LPT, PCMCIA, USB) або слот розширення материнської плати. Так само як такий пристрій можуть використовуватися смарт-карти (SmartCard).

Електронні ключі по архітектурі можна підрозділити на ключі з пам'яттю (без мікропроцесора) і ключі з мікропроцесором (і пам'яттю).

Найменш стійкими є системи з апаратною частиною першого типу. У таких системах критична інформація (ключ дешифрування, таблиця переходів) зберігається в пам'яті електронного ключа. Для дезактивації таких захистів у більшості випадків необхідно наявність у зловмисника апаратної частини системи захисту (перехоплення діалогу між програмною й апаратною частинами для доступу до критичної інформації).

Найбільш стійкими є системи з апаратною частиною другого типу. Такі комплекси містять в апаратній частині не тільки ключ дешифрування, але і блоки шифрування/дешифрування даних, у такий спосіб при роботі захисту в електронний ключ передаються блоки зашифрованої інформації, а приймаються відтіля розшифровані дані. У системах цього типу досить складно перехопити ключ дешифрування тому, що усі процедури виконуються апаратною частиною, але залишається можливість примусового збереження захищеної програми у відкритому виді після відпрацьовування системи захисту. Крім того, до них застосовні методи криптоаналізу.

Позитивні фактори захисту за допомогою електронних ключів: значне утруднення нелегального поширення і використання ПЗ, рятування виробника ПЗ від розробки власної системи захисту, висока автоматизація процесу захисту ПЗ, наявність API системи для більш глибокого захисту, можливість легкого створення демо-версій, досить великий вибір таких систем на ринку.

До негативних факторів відносяться: утруднення розробки і налагодження ПЗ через обмеження з боку систем захисту, додаткові витрати на придбання системи захисту і навчання персоналу, уповільнення продажів через необхідність фізичної передачі апаратної частини, підвищення системних вимог через захист (сумісність, драйвери), зниження відмовостійкості ПЗ, несумісність систем захисту і системного або прикладного ПЗ користувача, несумісність захисту й апаратури користувача, обмеження через несумісність електронних ключів різних фірм, зниження розширюваності комп'ютерної системи, утруднення або неможливість використання захищеного ПЗ в переносних і блокнотних ПК, наявність в апаратної частини розмірів і погроза крадіжки апаратного ключа.

Одним із найбільш перспективних методів захисту електронних ключів є використання динамічних кодів та пропрієтарних протоколів. Це дозволяє забезпечити унікальність переданих даних при кожній автентифікації користувача. Завдяки цьому, зчитавши дані при обміні (ці дії мають назву сніфінг), передавши ідентичні дані до зчитувача системи контролю і управління доступом, зловмисник не отримує результату у вигляді дозволу на прохід.

Можна зробити висновок, що зараз існує досить багато проблем із захистом програмного забезпечення, і тому розробляється велика кількість систем захисту програмного забезпечення, для їх подолання, без яких неможлива безпечна робота, як з програмним забезпеченням, так і з комп'ютером. Було розглянуто захист програмного забезпечення за допомогою електронних ключів та за результатами проведеного аналізу, виявлено найбільш перспективні методи для підвищення стійкості електронних ключів.