УДК 681.39

ПРОГРАМНИЙ ЗАСІБ ДЛЯ ЗАХИСТУ ВІД НЕСАНКЦІОНОВАНОГО ДОСЛІДЖЕННЯ

Швидкий М. П.
Науковий керівник – ст. викл. Каплун В. А.

Окрім проблем якості і надійності програмного забезпечення проблема його безпеки набуває все більшу актуальність. При цьому в рамках даної проблеми на перший план висувається безпека технологій створення програмного забезпечення комп'ютерних систем. Даний аспект проблеми безпеки програмних комплексів є порівняно новим і пов'язаний з можливістю впровадження в тіло програмних засобів на етапі їх розробки (або модифікації в ході авторського супроводу) так званих «програмних закладок». Крім того, при експлуатації програмних комплексів можливий певний алгоритм внесення програмного дефекту: дизасемблювання виконуваного коду, отримання початкового тексту, привнесення в нього деструктивної програми, повторна компіляція, корегування програми тощо. Саме це й обумовило створення програмного засобу для запобігання діям зловмисників різного роду.

Підсистема захисту від нелегального дослідження складається з ряду модулів, які здійснюватимуть захист від дизасемблювання та налагоджування за допомогою використання хуків, тобто перехоплення повідомлень системи та їх обробка до того, як вони досягнуть цільової віконної процедури. Механізм захисту обрано навісний, що позбавляє розробників від необхідності відволікатись на впровадження у код захищуваної програми елементів захисту. Тому у програмному засобі використовуються віддаленні хуки, які, як відомо, дозволяють перехоплювати події, що трапились в інших процесах. Крім того, передбачено антидампінговий захист, виконаний у вигляді окремого модуля. Цей модуль призначений для тимчасової модифікації exe-заголовку виконуваного модуля захищуваної програми, тобто заміни exe-заголовку при запуску програми (що не дозволить коректно зняти зліпок пам’яті – дамп) та повернення його до попереднього стану під час завершення програми і передачі керування операційній системі.

Таким чином, результатом розробки є програмний засіб, що складається із декількох модулів, які реалізовують навісний захист від несанкціонованого дослідження та модифікації методом використання хуків та антидампінгового захисту. Даний програмний засіб успішно може працювати окремо, але для підвищення ефективності захисту програм від зламу і дослідження їх зловмисниками він може бути складовою комплексного захисту програмного забезпечення.