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

АНАЛІЗ ПОКАЗНИКІВ ЕФЕКТИВНОСТІ ЗАСТОСУВАННЯ СИСТЕМ ЗАХИСТУ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Системи захисту програмного забезпечення (СЗПЗ) широко поширені і знаходяться в постійному розвитку, завдяки розширенню ринку програмного забезпечення і телекомунікаційних технологій. Необхідність використання систем захисту СЗПО обумовлена поруч проблем, серед яких варто виділити: незаконне використання алгоритмів, що є інтелектуальною власністю автора, при написанні аналогів продукту (промислове шпигунство); несанкціоноване використання ПО (крадіжка і копіювання); несанкціонована модифікація ПО з метою введення програмних зловживань; незаконне поширення і збут ПО (піратство). Орієнтовна структура наслідків неефективного забезпечення інформаційної безпеки в американських організаціях така : крадіжка конфіденційної інформації – 20-25% від загального річного збитку; фальсифікація фінансової інформації - 21-25%; зараження шкідливими програмами – 11-12%; порушення доступу до Web-сайтів – 1-11%; зрив роботи інформаційної системи – 4-10%; незаконний доступ співробітників до інформації – 4-9%; інші види шкоди – 14-33%.

Для захисту ПО використовується ряд методів, таких як:

Алгоритми заплутування – використовуються хаотичні переходи в різні частини коду, впровадження помилкових процедур – "пустушок", неодружені цикли, перекручування кількості реальних параметрів процедур ПО, розкид ділянок коду по різних областях ОЗУ і т.п.

Алгоритми мутації – створюються таблиці відповідності операндів – синонімів і заміна їх один на одного при кожному запуску програми за певною схемою або випадковим чином, випадкові зміни структури програми.

Алгоритми компресії даних – програма упаковується, а потім розпаковується в міру виконання.

Алгоритми шифрування даних – програма шифрується, а потім розшифровується у міру виконання.

Обчислення складних математичних виразів в процесі відпрацювання механізму захисту – елементи логіки захисту залежать від результату обчислення значення якої-небудь формули або групи формул.

Методи утруднення дизассемблирования – використовуються різні прийоми, спрямовані на запобігання дизассемблирования в пакетному режимі.

Методи утруднення налагодження – використовуються різні прийоми, спрямовані на ускладнення налагодження програми.

Емуляція процесорів і операційних систем – створюється віртуальний процесор і / або операційна система (не обов'язково реально існуючі) і програма-перекладач із системи команд IBM в систему команд створеного процесора або ОС, після такого перекладу ПО може виконуватися тільки за допомогою емулятора, що різко ускладнює дослідження алгоритму ПО.

Нестандартні методи роботи з апаратним забезпеченням – модулі системи захисту звертаються до апаратури ЕОМ, минаючи процедури ОС, і використовують маловідомі або недокументовані її можливості.

Немає сумнівів, що захист критично важливих для власників інформаційних систем відповідає численним міжнародним, національним, корпоративним, нормативним і методичним документам. Застосовуються досить дорогі технічні засоби і впроваджуються строго регламентовані організаційні заходи. Однак немає відповіді на найважливіше питання – наскільки пропоноване або вже реалізоване рішення добре, яка його планована або реальна ефективність.

Поява міжнародного стандарту ОК є якісно новим етапом у розвитку нормативної бази оцінки безпеки ІТ. Порівняння оцінок здійснюється за допомогою загального переліку (набору) вимог для функцій захисту продуктів і систем, а також методів точних вимірювань, які проводяться під час отримання оцінок захисту. Грунтуючись на цих вимогах, в процесі вироблення оцінки рівня захисту встановлюється рівень довіри.

Ефективність захисних заходів (ЗМ) повинна оцінюватися на стадії проектування, для отримання найкращих показників працездатності системи в цілому.

У загальному випадку ефективність ЗМ оцінюється як на етапі розробки, так і в процесі експлуатації системи захисту. В оцінці ефективності ЗМ, в залежності від використовуваних показників і способів їх отримання, можна виділити три підходи:

– класичний;

– офіційний;

– експериментальний.

При розробці і аналізі захисту програмного забезпечення необхідно враховувати існуючу законодавчу базу, при цьому потрібно проводити детальний економічний аналіз ситуації, застосовуючи різні критерії оцінки, а потім створювати стратегію захисту, що включає застосування технічних і організаційних заходів захисту програмного забезпечення.