Захист програм та даних в комп'ютерних системах і мережах

УДК 004.056.5

В.А. Бісюк[1]
Кіровоградський національний технічний університет

Перспективи розробки і впровадження комбінованих систем захисту інформації

Із становленням України як незалежної держави, перебудовою таких галузей, як економіка та обороноздатність, гостро постала проблема створення та впровадження принципово нових власних систем захисту (СЗ) інформації, зокрема в програмному забезпеченні (ПЗ) керування автоматизованими та комп'ютерними системами.

Програмне забезпечення, що використовується в сучасних великих розподілених системах (особливо в тих, що мають вихід в зовнішні мережі) може піддаватися різного роду атакам (комп'ютерні віруси, ddos атаки і т.д.) тому питання пошуку найбільш ефективних систем захисту ПЗ стоїть досить гостро.

Системи захисту програмного забезпечення по методу установки і впровадження можна розділити на:

1) системи, що встановлюються на скомпільовані модулі ПЗ;

2) системи, що вбудовуються (інтегруються) у програмний код до компіляції;

3) комбіновані.

Аналіз останніх джерел та наукових публікацій показав, що:

- Перший тип систем захисту найбільш зручний і простий для розробки і використання. Таку СЗ можна легко модифікувати і захистити вже цілком готове й протестоване ПЗ, тому такий тип СЗ найбільш популярний. Але стійкість цих СЗ досить низька, тому що для обходу захисту достатньо визначити точку завершення роботи «конверта» захисту і передачі керування захищеній програмі, а потім примусово зберегти її в незахищеному виді.
- Процес розробки і тестування ПЗ з системою захисту другого типу стає складнішим, зменшується його надійність, тому що, крім самого ПЗ, помилки може містити API системи захисту або процедури, які його використовують. Але такі системи є більш стійкими до атак, тому що тут зникає чітка границя між системою захисту і як таким ПЗ, відповідно «нападникам» значно складніше відокремити і «нейтралізувати» таку СЗ.
- Найбільш стійкими вважаються комбіновані системи захисту. Вони максимально ускладнюють аналіз і дезактивацію своїх алгоритмів, але є найбільш складними в реалізації.

Отже, проведені дослідження показали, що найбільш перспективним є інтегрування системи захисту в програмне забезпечення на етапі компіляції і додавання зовнішніх модулів для захисту.

---

[1] викладач кафедри програмного забезпечення