РЕКОМЕНДАЦІЇ ЩОДО ВИЯВЛЕННЯ І ПРОТИДІЇ ПРОГРАМНИХ ЗАКЛАДКАМ В РІЗНИХ ОПЕРАЦІЙНИХ СИСТЕМАХ

Верховець О.С.
ДержНДІ технологій кібербезпеки та захисту інформації, Київ
Науковий керівник – Гнатюк С.О., д.т.н., доцент

Виробники не гарантують відсутність в обладнанні та програмному забезпеченні (ПЗ) апаратно-програмних закладок, комп'ютерних вірусів та інших недокументованих можливостей, що можуть зашкодити роботі системи. Одним з аргументів відмови від гарантій відсутності закладок є наявність механізму впровадження програмних закладок за допомогою інструментальних засобів розробки та налагодження програм на етапі розроблення ПЗ. Виявлення закладок такого типу є дуже складним, тому метою дослідження є аналіз особливостей застосування та ідентифікації програмних закладок у різних ОС.

Програмні закладки обумовлені тим, що вони можуть вносити довільні спотворення до початкового коду програми, яка знаходиться в оперативній пам'яті комп'ютерної системи (КС), здійснювати перенесення інформації з однієї області оперативної або зовнішньої пам'яті КС до іншої, спотворювати інформацію, що виводиться на інші пристрої або до каналу зв'язку отриману в результаті роботи інших програм. До основних властивостей програмних закладок доцільно віднести: виконання операцій запису та зчитування з пам'яті КС; внесення довільних перекручувань в коди програм, які знаходяться в оперативній пам'яті КС; перенесення інформації з одних областей пам'яті КС в інші; спотворювання інформації, отриманої в результаті роботи інших програм, яка виводиться на пристрої КС або до каналу зв'язку.

Виходячи з викладеного можна сформулювати такі рекомендації:

1. Пошук та нейтралізація програмних закладок дуже трудомісткий процес, який потребує багато часу та ресурсів. Це потрібно врахувати під час реалізації заходів захисту.
2. Підходи до виявлення програмних закладок в кожному конкретному випадку повинні визначатися окремо. Уніфікувати процес пошуку та нейтралізації програмних закладок на практиці майже неможливо.
3. Розробка уніфікованого засобу пошуку програмних закладок призначених для будь-якого ПЗ певної КС практично не можлива і як наслідок недоцільна.

Список використаних джерел:

1. Максименко А.А., Козюра В.Д. Програмні закладки та методи захисту комп'ютерних систем від них, *Актуальні проблеми управління інформаційною безпекою держави,* 2019, с. 329.
2. Савенко О.С. Моделі незадокументованих закладок програмного забезпечення в локальних комп'ютерних мережах, *Вимірювальна та обчислювальна техніка в технологічних процесах,* Том 2, 2019, с. 84-90.