

РОЗРОБКА АНТИВІРУСНОЇ СИСТЕМИ НА БАЗІ ПОВЕДІНКОВОГО АНАЛІЗУ

*канд. техн. наук, доц. С.Ю. Гавриленко, аспірант І.В. Шевердін,
Національний технічний університет "Харківський політехнічний
інститут", м. Харків*

У доповіді проаналізовано проблему захисту від несанкціонованого доступу [1 – 3]. Запропоновано розробку антивірусного програмного додатку, базуючись на концептуальних принципах обробки системних подій операційної системи.

Для збору подій було використано програмний додаток "Process Monitor", для аналізу зібраної статистики – додаток "Deductor Studio Academic". Промодельована робота вірусів сімейства Trojan. Проаналізовано події вірусних команд та зібрано статистику. Для подальшого аналізу використано наступні поля подій операційної системи Windows 10: Process Name, Result, Image Path, Event Class, Company, Version, Authentication ID, Category.

Аналіз різниці роботи інфікованої та не інфікованої операційної системи показав:

- модифікацію реєстру;
- зміни в головному завантажувальному записі MBR;
- зростання кількості відмов у доступі до файлу;
- зростання кількості системних подій: видалення, модифікації чи створення файлів;
- збільшення кількості операцій з системним реєстром;
- збільшення кількості операції запису та зчитування метаданих;
- відсутність версій та підписів в шкідливих програмних додатках;
- збільшення кількості подій системного сервісу, який був використаний у якості ідентифікатора запуску шкідливого процесу.

Список літератури: 1. Експерт: Україна зазнає кібератаки 24 години на добу РІА Новини України 2017 [Електронний ресурс]. – Режим доступу до ресурсу: <http://rian.com.ua/interview/20171027/1028904288/ukraine-kiberataki.html>. 2. Кіберполіція повідомила про наслідки вірусу BadRabbit для України РІА Новини України 2017 [Електронний ресурс]. – Режим доступу до ресурсу: <http://rian.com.ua/incidents/20171025/1028863477.html>. 3. Удосконалена концепція захисту даних на базі багаторівневого аналізу карт операційної системи / С.Ю. Гавриленко, І.В.Шевердін // Системи управління навігації та зв'язку. – Полтава, – 2017. – С. 8.