А. А. Шамрей

(УО «ГрГУ им. Я. Купалы», Гродно)

**ПРОЕКТИРОВАНИЕ АВТОМАТИЗИРОВАННОГО
СРЕДСТВА ДЛЯ ОБНАРУЖЕНИЯ УГРОЗ ВРЕДОНОСНОГО
ПО С ИСПОЛЬЗОВАНИЕМ ИЗОЛИРОВАННОЙ СРЕДЫ**

Целью работы является спроектировать автоматизированное средство для обнаружения угроз вредоносного программного обеспечения с использованием изолированной среды.

Материалы XXII Республиканской научной конференции студентов и аспирантов «Новые математические методы и компьютерные технологии в проектировании, производстве и научных исследованиях», Гомель, 25 – 27 марта 2019 г.

Благодаря использованию данного средства будет обеспечена безопасность компьютеров пользователей или компаний.

Всем известно об опасности заражения вредоносными программами из Интернета в наши дни. Опасность всегда была там, но сейчас она увеличилась как никогда ранее, потому что люди с зловредными намерениями постоянно разрабатывают новые методы для заражения систем, а самые неопытные пользователи наиболее подвержены этому воздействию. Инфекция вредоносных программ из Интернета может произойти по-разному, некоторые из которых:

- загрузка зараженной программы/файла с вредоносного сайта;
- серфинг вредоносных сайтов и др.

Самой главной частью любого создаваемого автоматизированного программного обеспечения является «движок» – это модуль, который отвечает за проверку объектов и детектирование вредоносного программного обеспечения. Именно от «движка», от того, как он написан, какие он использует методы обнаружения и эвристики, зависит качество детектирования вредоносного программного обеспечения и, как следствие, уровень защиты.

Анализ компьютерных вирусов имеет некоторые общие закономерности, которые обеспечивают эффективность процесса анализа.