УДК 004.4

***А.В. ДЕРКАЧ***, НТУ «ХПИ», Харьков, Украина
***С.Ю. ГАВРИЛЕНКО***, канд. техн. наук, проф., НТУ «ХПИ», Харьков, Украина

## Разработка эвристического анализатора для обнаружения вредоносного программного обеспечения

Эвристический анализ предполагает, что новые вирусы часто оказываются похожи на какие-либо из уже известных.

Основанный на таком предположении эвристический метод заключается в поиске файлов, которые очень близко похожи на сигнатуры известных вирусов.

Преимуществом данного метода является возможность обнаруживать неизвестные ранее вредоносные программы, даже если они не очень похожи на уже известные [1].

Например, новая вредоносная программа может использовать для проникновения на компьютер новую уязвимость, но после этого начинает выполнять уже привычные вредоносные действия.

Анализатор кода антивируса проверяет исследуемую программу в процессе эвристического анализа.

Антивирус считывает инструкции в свой буфер, разбирает их и исполняет по одной.

После этого анализатор кода вычисляет контрольную сумму и сравнивает с хранимой в базе.

Процесс продолжается пока часть вируса, которая необходима для подсчета контрольной суммы, не будет расшифрована [2].

Недостатком эвристического анализа является то, что при успешном определении, лечение неизвестного вируса является практически невозможным.

В виде исключения, возможно лечение однотипных и полиморфных зашифрованных вирусов, не имеющих постоянного вирусного тела, но использующих единую методику внедрения.

**Список литературы**:

**1.** *Латыпов Н.Н.* Инженерная эвристика / *Н.Н. Латыпов, С.В. Ёлкин, Д.А. Гаврилов*. – М.: Астрель, 2012.

**2.** *Климентьев К.* Компьютерные вирусы и антивирусы. Взгляд программиста / *К. Климентьев*. – М.: ДМК, Пресс, 2013 г.