

## СЕКЦИОННЫЕ ДОКЛАДЫ

### СЕКЦИЯ "ПРОБЛЕМЫ МОДЕЛИРОВАНИЯ"

#### **ЭВРИСТИЧЕСКИЙ АНАЛИЗАТОР ВРЕДНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ**

*к.т.н., доц. С.Ю. Гавриленко, студ. А.В. Деркач, НТУ "ХПИ", г. Харьков.*

Эвристический анализ основывается на предположении, 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 соответствуют сигнатурам 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 использоваться для проникновения на компьютер, после чего начнет выполнять свои действия.

Анализатор кода антивируса проверяет исследуемую программу во время эвристического анализа. Антивирус считывает инструкции в буфер, разбирает их и исполняет по одной. После этого анализатор кода вычисляет контрольную сумму и сравнивает с хранимой в базе.

Недостатком эвристического анализа является то, что при успешном определении, лечение неизвестного вируса является практически невозможным. Как исключение, возможно лечение однотипных и полиморфных шифрующихся 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.