ления в объеме каучуковой матрице, что в дальнейшем положительно отражается на свойствах получаемых вулканизатов.

ЭВРИСТИЧЕСКИЙ АНАЛИЗ КАК ИНСТРУМЕНТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Цветков В.Я., Булгаков С.В.
Московский государственный университет геодезии и картографии
Москва, Россия

В настоящее время информационные угрозы постоянно расширяются. Появляются так называемые киберугрозы и кибератаки. В информационной безопасности появилось новое направление цифровая безопасность (Digital security) цифровая защита (Digital protection) . Это определяет актуальность развития таких методов. Одной из широко распространенных информационных (цифровых) угроз являются компьютерные вирусы. Многие средства информационной безопасности в качестве цифрового метода защиты применяют технологию эвристического анализа программного кода. Эвристический анализ нередко используется совместно с сигнатурным сканированием для поиска сложных шифрующихся и полиморфных вирусов.

В процессе эвристического анализа используется эмулятор кода и производится проверка эмулируемой программы анализатором кода. Например, программа может быть инфицирована полиморфным вирусом, состоящим из зашифрованного тела и расшифровщика.

Эмулятор кода эмулирует работу данного вируса по одной инструкции, после этого анализатор кода подсчитывает контрольную сумму и сверяет ее с той, которая хранится в базе. Эмуляция будет продолжаться до тех пор, пока необходимая для подсчета контрольной суммы часть вируса не будет расшифрована. Если сигнатура совпала — программа идентифицирована.

Другим распространённым методом эвристического анализа, применяемым большой группой антивирусов, является декомпиляция подозрительной программы и анализ её исходного кода. Исходный код подозрительного файла проходит сверку и сравнение с исходным кодом известных вирусов и образчиков вирусной активности. В случае, если определённый процент исходного кода идентичен коду известного вируса или вирусной активности, файл отмечается как подозрительный, о чем оповещается пользователь

Методика эвристического анализа позволяет обнаруживать ранее неизвестные инфекции, однако, лечение в таких случаях практически всегда оказывается невозможным. В таком случае, как правило, требуется дополнительное обновление антивирусных баз для получения последних сигнатур и алгоритмов лечения, которые, возможно, содержат информацию о ранее неизвестном вирусе. В противном случае, файл передается для исследования антивирусным аналитикам или авторам антивирусных программ

Методы эвристического сканирования не обеспечивают какой-либо гарантированной защиты от новых, отсутствующих в сигнатурном наборе компьютерных вирусов, что обусловлено использованием в качестве объекта анализа сигнатур ранее известных вирусов, а в качестве правил эвристической верификации — знаний о механизме полиморфизма сигнатур. В то же время, поскольку этот метод поиска базируется на эмпирических предположениях, полностью исключить ложные срабатывания нельзя

Чрезмерная подозрительность эвристического анализатора может вызывать ложные срабатывания при наличии в программе фрагментов кода, выполняющего действия и/или последовательности, в том числе и свойственные некоторым вирусам. В частности, распаковщик в файлах, запакованных PE-упаковщиком (Win)Upack вызывает ложные срабатывания целого ряда антивирусных средств, де-факто не признающих такой проблемы.

Наличие простых методик обмана эвристического анализатора. Как правило, прежде чем распространять вредоносную программу (вирус), ее разработчики исследуют существующие распространенные антивирусные продукты, различными методами избегая ее детектирование при эвристическом сканировании. К примеру, видоизменяя код, используя элементы, выполнение которых не поддерживается эмулятором кода данных антивирусов, используя шифрование части кода и др.

Тем не менее, несмотря на недостатки, данный подход используется и имеет перспективу развития. Одним из побочных методов применения данного метода является цифровая защита авторских прав. Наряду со стеганографическими методами эвристический метод позволяет выявлять цифровые знаки авторского права.