ИДЕНТИФИКАЦИЯ АВТОРА ЭЛЕКТРОННОГО ПРОДУКТА

С.А. ТЫКОЦКИЙ

Проблема идентификации автора вредоносного кода и доказательство принадлежности кода определенному автору — главная задача нашего исследования.

Вирусы, "трояны", взлом программного обеспечения с каждым годом наносят все больший урон компьютерной индустрии. Как найти виновного? Как доказать его вину? Типичными уликами, остающимися после атаки, является исполняемый модуль или исходный код. Оба случая требуют различного подхода при их анализе.

В работе проведены исследования по определению характерных признаков электронных продуктов на примере исходных кодов программ и исполняемых модулей. Лингвистическая и стилистическая составляющие являются наиболее показательными для статистического анализа, позволяют наиболее точно идентифицировать субъекта. Сама же идентификация производится не по одному из признаков, а по их совокупности.

В случае работы с исходными кодами мы имеем достаточно большие возможности для идентификации автора. Отождествление может быть осуществлено по следующим признакам, которые различны для каждого субъекта: форматирование исходного кода, стиль написания комментариев, именование переменных, грамматические ошибки при объявлении переменных и написании комментариев, степень владения автора возможностями языка программирования, использование нулевых ветвей

в коде программы, типичные ошибки, допущенные при кодировании программы.

В случае работы с исполняемыми модулями возможности анализа заметно сокращаются, вследствие преобразования исходного кода на стадии компиляции. Однако и в данном случае существуют методы и характеристики, позволяющие идентифицировать автора: анализ структур данных и алгоритмов, ошибки, допущенные при разработке, системные вызовы, уровень знания языка программирования и операционной системы, компилятор, используемый при сборке исполняемого модуля.

Исследования, в области идентификации автора электронного продукта, сталкиваются с рядом проблем. Довольно часто, при разработке программного обеспечения, используется чужой код или же разработку проекта ведет группа программистов. Разработчик может преднамеренно вносить искажения в исходный код. Размер кода, необходимый для объективного анализа принадлежности его автору остается достаточно субъективной величиной. Среда разработки также в некоторой степени нивелирует стилистические различия в написании кода разными авторами. Несмотря на все это, остается достаточное количество признаков, по которым возможна идентификация автора электронного продукта.