УДК 004.4'242

ДОСЛІДЖЕННЯ МЕТОДІВ ДЕОБФУСКАЦІЇ ПРОГРАМНОГО КОДУ

В. Є. Фейцер [1], *В. І. Панченко*[2]

[1] *магістрант кафедри Обчислювальної техніки та програмування, НТУ «ХПІ», Харків, Україна*

[2] *старший викладач кафедри Обчислювальної техніки та програмування, НТУ «ХПІ», Харків, Україна*

feysaball123@gmail.com

Актуальність роботи полягає в тому, що інколи в компаніях, які займаються розробкою програм, за різними обставинами втрачають початкові коди програм, які вони хотіли б змінити, або замовник надає застарілу програму, яку необхідно оновити. За умови використання програм, які написані інтерпретованими мовами програмування, часто використовують обфускацію (заплутування) коду для захисту від несанкціонованого втручання в вихідний код програми. Не дивлячись на те, що обфускований код можна розібрати, але на це потребує значних витрат часу та напруженої роботи фахівців..

Метою роботи є дослідження методів деобфускації інтерпретованих язиків і розробка програми, яка буде деобфусковувати код до початкового або до зручного до аналізу стану.

Для досягнення зазначеної мети в роботі були поставлені наступні завдання:

- дослідити існуючі методи обфускації;
- обрати найпоширеніші методи обфускації із досліджених;
- створити програму, яка зможе деобфусковувати заплутаний код по вибраному із досліджених методів.

На основі досліджених методів було визначено, що одним з найпоширеніших методів обфускації є метод видалення токенів (видалення коментарів, пробілів, символів горизонтальної та вертикальної табуляції, символів переносу рядка та символів переносу сторінки). Головне завдання цього методу – зробити код програми нечитабельним. Маючи уяву про те, як саме працює обфускація, було виявлено, на основі яких методів та регулярних виразів потрібно створити програму для деобфускації коду.

Результатом роботи є програма, яка працює під керівництвом операційної системи Microsoft Windows та яка приймає на вхід обфускований за допомогою метода видалення токенів код, та на виході видає код в початковому вигляді, сприятливому для читання та редагування. Розроблена програма є частиною дипломної роботи на здобуття ступеню магістра з комп'ютерної інженерії.

Список літератури:

1. Yadegari B., Johannesmeyer B., Whitely B., Debray S. A generic approach to automatic deobfuscation of executable code / B. Yadegari, B. Johannesmeyer, B. Whitely, S. Debray. – IEEE Symposium Security and Privacy (S&P). – 2014. – 18 p.

2. Lu G., Debray S. Automatic Simplification of Obfuscated JavaScript Code: A Semantics-Based Approach / G. Lu, S. Debray. – Proc. ICISTM-12 Workshop on Program Protection and Reverse Engineering (PPREW), – 2012. – 10 p.