

## МЕТОДИ ЛЕКСИЧНОЇ ОБФУСКАЦІЇ ПРОГРАМ НА ОСНОВІ ШИФРУВАННЯ

Вінницький національний технічний університет

**Анотація:** У даній роботі представлено метод лексичної обфускації, який ґрунтується на використанні буквеного генератора. Описано підхід, який покращить стійкість обфускованих програмних засобів до зламу.

**Ключові слова:** обфускація, деобфускація, декомпілятор, дизасемблер.

**Abstract:** This paper presents a method of lexical obfuscate which is based on using alphabetic generator. The approach, which improves infeasibility of obfuscated software, is presented.

**Key words:** obfuscate, deobfuscate, decompiler, disassemblers.

Поширеність піратства обумовлюється недостатньою стійкістю програмних засобів до зламу, якщо в ньому немає відповідного захисту, пірати можуть скопіювати програми та неліцензійно їх поширювати. Однією із великих компаній, які зазнали краху, від піратства є Black Isle Studios, що займалась розробкою комп'ютерних ігор [1]. Таким чином, питання захисту програмного забезпечення від несанкціонованого копіювання, поширення й використання є одним з найбільш важливих у комп'ютерній практиці.

Одним із методів захисту програмних засобів від піратства є обфускація (заплутування програмного коду). Недоліком обфускації є те, що більшість із відомих методів сповільнюють роботу програм та легко піддаються декомпіляторам і дезасемблерам.

Метою є підвищення стійкості обфускації до атак на програмні засоби.

Для створення ефективного обфускатора здійснено аналіз наведених методів обфускації [2] лексичної, обфускації даних, обфускації зберігання та обфускації непрозорих предикат. Проаналізувавши методи, слід звернути увагу на лексичну обфускацію, адже при обфускуванні даних, не вимагається використання додаткових дій, які б сповільнювали процес виконання обфускованої програми. Пропонується покращення лексичної обфускації, шляхом подолання проблеми заміни за конкретним алфавітним розташуванням, що піддається декомпіляторам та дезасемблерам.

Надійність лексичної обфускації пропонується використання буквеного генератора, який виконуватиме заміну, наприклад таку, яка наведена на рис.1.



Рисунок 1 – Заміна з використанням буквеного генератора

Для покращення запропоновано використовувати набір алфавітних таблиць, а номер таблиці, яка повинна використовуватись на  $i$ -й ітерації визначати на основі згенерованих генератором псевдовипадкової послідовності, представленою у такому вигляді:

$$r_i = rand * (r_{i-1}),$$

де  $r_i$  — кількість таблиць, які використовувати для заміни.

Отримані значення  $n$  згенерованих таблиць матимуть такий вигляд рис.2.

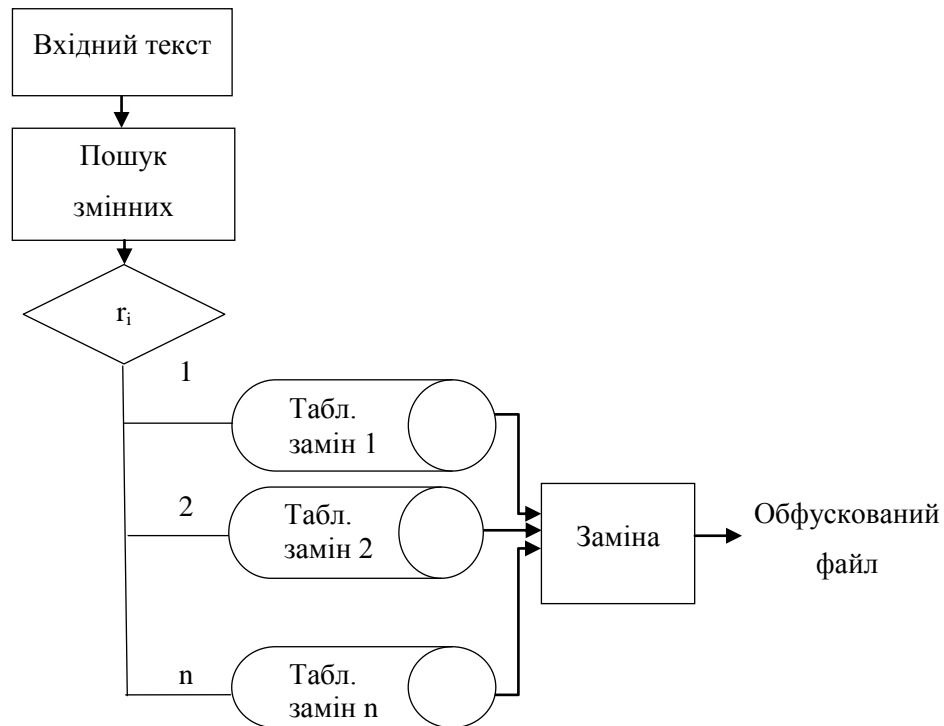


Рисунок 2 – Фрагмент алгоритму обфускації

Використання згенерованих таблиць поліпшить захищеність програмних засобі, оскільки заміна відбуватиметься щоразу випадковою послідовністю, це сприятиме значному забілюванню даних, обфускований програмний засіб не піддаватиметься декомпіляторам та дизасемблерам, що значно ускладнить використання піратства.

### СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. L.Cheong Game Info. Lionheart Chronicles / L.Cheong // GameSpy – Режим доступу: - <http://www.ign.com>.
2. C. Colleberg Taxonomy of Obfuscating Transformation./ C. Colleberg, C. Thomborson// Department of Computer Science, The University of Auckland, 1997 – 56р. - Режим доступу: <http://www.cs.arizona.edu/colleberg/Research/Publications/Collberg>.
3. А. В. Чернов Анализ запутывающих преобразований программ / Библиотека аналитической информации 2003. С. 24-26 с. — Режим доступу : <http://www.citforum.ru/security/articles/analysis/>.
4. Ю.М. Лифшиц Запутывание (обфускация) программ /Обзор. СПб. отд. Мат. Инст. Им. В. А. Стеклова РАН, 2004 - Режим доступа: <http://logic.pdmi.rac.ru/~yura/of/survey1.pdf>.

**Мазур Ірина Вікторівна** факультет інформаційних технологій та комп'ютерної інженерії, студент групи BS-126, Вінницький національний технічний університет, Вінниця, [irkamazur88@gmail.com](mailto:irkamazur88@gmail.com).

**Баришев Юрій Володимирович** кандидат технічних наук, доцент кафедри захисту інформації, Вінницький національний технічний університет, Вінниця, [yuriy.baryshev@gmail.com](mailto:yuriy.baryshev@gmail.com).

**Mazur Iryna** faculty of Information Technologies and Computer Engineering, student group BS-12b, Vinnytsya National Technical University, Vinnytsya, [irkamazur88@gmail.com](mailto:irkamazur88@gmail.com).

**Baryshev Yuriy** ph.d Vinnytsya National Technical University, Vinnytsya, [yuriy.baryshev@gmail.com](mailto:yuriy.baryshev@gmail.com).