**Лабораторная работа №6**

**Защита ПО от несанкционированного использования**

Количество часов практических занятий – 6

Количество часов самостоятельной работы – 10

**Цель работы:** Познакомиться с основными технологиями защиты программного обеспечения от несанкционированного использования.

Получить навыки защиты разработанной программы от несанкционированного копирования.

**ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ**

В результате выполнения лабораторной работы №5 были созданы web-приложения, обеспечивающие аутентификацию пользователей, с разделяемым доступом к информационным ресурсам, которые обеспечивают защиту от основных удаленных атак.

Вместе с тем для любых коммерческих приложений не менее актуальным является решение задачи защиты авторских прав разработчика либо пользователя системы.

Одним из основных способов защиты авторских прав разработчика **является запутывание (obfuscated) или обфуксация программного кода.**

**Обфуска́ция** (от лат. *obfuscare* — затенять, затемнять; и англ. *obfuscate* — делать неочевидным, запутанным, сбивать с толку) или **запутывание кода** — приведение исходного текста или исполняемого кода программы к виду, сохраняющему её функциональность, но затрудняющему анализ, понимание алгоритмов работы и модификацию при декомпиляции.

Обфуксация производится в следующих целях:

1. Затруднение декомпиляции/отладки и изучения программ с целью обнаружения функциональности.
2. Затруднение декомпиляции пропритарных программ с целью предотвращения обратной разработки или обхода DRM и систем проверки лицензий.
3. Оптимизация программы с целью уменьшения размера работающего кода и (если используется некомпилируемый язык) ускорения работы.
4. Демонстрация неочевидных возможностей языка и квалификации программиста (если производится вручную, а не инструментальными средствами).

«Запутывание» кода может осуществляться на уровне алгоритма, исходного текста и/или ассемблерного текста. Для создания запутанного ассемблерного текста могут использоваться специализированные компиляторы, использующие неочевидные или недокументированные возможности среды исполнения программы. Существуют также специальные программы, производящие обфускацию, называемые **обфускаторами** (англ. *obfuscator*).

Описание запутывающих преобразований приведено **в приложении.**

**ЗАДАНИЕ:**

1. Реализовать на выбор 3 метода обфуксации программного кода приложения, разработанного в рамках лабораторных работ 4,5, позволяющие защитить ПО от несанкционированного использования в следующих комбинациях:

* По одному.
* Любые 2 на выбор из трех одновременно.
* Все три одновременно.

1. Протестировать работоспособность приложения с запутанным программным кодом.
2. Проверить и пояснить следующие свойства, которым должна удовлетворять запутанная программа:

* Запутывание должно быть *замаскированным*. То, что к программе были применены запутывающие преобразования, не должно бросаться в глаза.
* Запутывание не должно быть регулярным. Регулярная структура запутанной программы или её фрагмента позволяет человеку отделить запутанные части и даже идентифицировать алгоритм запутывания.