УДК 004.056.55

WHITE-BOX КРИПТОГРАФИЯ

И.В. Камнев (Национальный исследовательский университет ИТМО, г. Санкт-Петербург)
Научный руководитель – А.Б. Левина (Национальный исследовательский университет ИТМО, г. Санкт-Петербург)

В работе будет осуществлён обзор не так широко известного метода защиты приложений – white-box криптография. Показаны её основные принципы, противоречия и проблемы. Осуществлён обзор методов определения сильных и слабых white-box решений, показаны возможные методы модернизации этого метода.

Введение. В настоящее время метод криптографического преобразования информации используется повсеместно, однако, при том что сам алгоритм не имеет открытых на данный момент уязвимостей, он будет выполнять возложенные на него функции только при условии, что среда его выполнения является защищённой и злоумышленник будет иметь доступ только к описанию алгоритма. Поэтому необходимо использовать методы защиты кода с сохранением конфиденциальности данных при получении доступа к алгоритму злоумышленником.

Основная часть. White-box криптография позволяет использовать приложения в не доверительных средах с максимально возможным сохранением конфиденциальности. White-box криптографией можно назвать метод запутывания, предназначенный для реализации криптографических примитивов таким образом, что даже злоумышленник, имеющий полный доступ к реализации и платформе выполнения, не может извлечь ключ шифрования. Однако у этого метода есть определённый набор проблем, для минимизации которых необходимо разрабатывать необходимые методы, которые разрабатываются корпорациями, которые используют методы White-box криптографии для защиты контента.

Выводы.
Разработка более совершенных методов White-box криптографии позволяет повысить защищённость приложений от атак по сторонним каналам, и их использование повышает защищенность системы от действий злоумышленника.

Авторы _____/Камнев И.В.

Научный руководитель _____/Левина А.Б.