МЕТОДЫ ЗАЩИТЫ АВТОРСКОГО ПРАВА НА ПРОГРАММНЫЕ ПРОДУКТЫ С ПОМОЩЬЮ ВОДЯНЫХ ЗНАКОВ И ОТПЕЧАТКОВ ПАЛЬЦЕВ

Шулицкий Д.С.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Ярмолик В.Н. – д.т.н.,профессор

Защита цифровых работ от нелегального использования и распространения является сложной задачей в информационном обществе. Полное предотвращение незаконного использования работ недостижимо за разумную цену. Большинство схем защиты авторского права отпугивают людей от нелегального использования и распространения цифрового контента тем, что позволяют обнаружить незаконное использование. Для этого в оригинальную работу добавляют идентификационную информацию с помощью техники водяных знаков или отпечатков пальцев.

Цифровой водяной знак – это информация, внедрённая в цифровую работу, которая позволяет автору работы доказать своё авторство. В самом простом случае водяной знак представляет собой строку, указывающую, что данная работа охраняется авторским правом. Цифровой отпечаток пальца является водяным знаком, в котором содержится не только информация об авторе, но и о субъекте, которому предоставлено право пользования произведением [1].

Если функция извлечения водяного знака общедоступна, водяной знак называют видимым. Если эта функция доступна только лицу, внедрившему цифровой водяной знак, его называют невидимым.

Водяные знаки в программном обеспечении можно разделить на водяные знаки данных и водяные знаки кода, а также на статические и динамические. Водяные знаки данных размещаются в неиспользуемых структурах данных программы. Водяные знаки кода внедряются при помощи манипуляций с инструкциями микропроцессора. Статические водяные знаки извлекаются непосредственно из файла программы. Для извлечения динамических водяных знаков необходим запуск программы и получение результата её работы [2].

Цифровые отпечатки пальцев, в отличие от обычных водяных знаков, содержат не только информацию об авторе программы, но и информацию о покупателе программы. При продаже очередной цифровой копии программы формируется содержимое отпечатка пальца. Далее эта информация зашифровывается при помощи приватного ключа разработчика. Это позволяет доказать, что цифровой отпечаток пальца был внедрён конкретным лицом. Затем отпечаток пальца внедряется в программное обеспечение. Отпечатки пальца позволяют обнаруживать источники нелегального распространения программы, так как не составляет труда определить покупателя конкретной копии программы.

К цифровым отпечаткам пальцев предъявляются дополнительные требования по сравнению с водяными знаками: даже если атакующий имеет доступ к некоторому количеству копий программы, он не должен иметь возможность прочесть, повредить или удалить отпечаток пальца на основе информации, полученной путём сравнения копий.

Концептуальной проблемой обычных водяных знаков является то, что демонстрация присутствия водяного знака как свидетельства раскрывает чувствительную информацию, которая может быть использована для удаления водяного знака. Желательно убедить верификатора в том, что водяной знак присутствует и не раскрыть ему информацию, которая может помочь удалить водяной знак. Одним из подходов к решению данной проблемы является использование слепой проверки водяных знаков. Слепые протоколы позволяют убедить верификатора, что правообладатель знает секретное значение, и верификатор не узнаёт ничего нового о секретных данных правообладателя. Например, правообладатель может создать настоящий водяной знак и спрятать его в большом списке поддельных водяных знаков. Затем он предлагает верификатору обнаружить все водяные знаки и доказывает, что, по крайней мере, один из водяных знаков является настоящим, не раскрывая, какой именно. Безопасность данного метода основана на том, что количество водяных знаков в списке должно быть на столько большим, что невозможно удалить их все без серьёзного ухудшения стего-данных [3].

Список использованных источников:

1. Криптография, стеганография и охрана авторского права / В.Н.Ярмолик, С.С. Портянко, С.В.Ярмолик / Издательский центр БГУ — Минск, 2007. — С. 195–211

2. Watermarking, Tamper-Proofing and Obfuscation – Tools for Software Protection / C. Collberg, C. Thomborson – Department of Computer Science University of Arizone, 2000. – P. 7-11.

3. Zero-Knowledge Watermark Detection and Proof of Ownership / A. Adelsbach, A. Sadeghi – LNCS, 2001. – P. 273-288.