КРИПТОГРАФИЧЕСКИЕ ПРОЦЕДУРЫ СОЗДАНИЯ И ВЕРИФИКАЦИИ ИДЕНТИФИКАТОРОВ ДОКУМЕНТОВ И ТОВАРОВ

В.Ю. Липень

В докладе автор анализирует различные методы и средства защиты бумажных документов от фальсификации и системы контроля за обращением документов. Отдельно рассматриваются методы защиты бланков строгой отчетности (полиграфия, спецкраски, голограммы, муаровые изображения и др.) и методы защиты контента (специальные реквизиты, шифрование, печать защитных данных, например, электронной цифровой подписи (ЭЦП) и открытого ключа в виде двумерного штрих-кода (ШК) и др.). Анализируются патенты и публикации, обосновывающие использование графической интерпретации ЭЦП в виде двумерного ШК. Рассматривается не очень успешный опыт создания и эксплуатации Единый Государственный автоматизированный системы (ЕГАИС), которая предназначена для компьютерного контроля изготовления и обращения алкогольной продукции в России. Анализируются аналогичные подходы к защите документов, предлагаемые в рассмотренных патентах.

Одним из выявленных недостатков подхода, реализованного в ЕГАИС, является необходимость размещения на этикетке товара графического образа ЭЦП и открытого ключа в виде двумерного ШК, что предполагает необходимость печати, оптического считывания и верификации оригинальных ШК (например, PDF-417), имеющих емкость более килобайта.

Еще в 2002 г. автором предлагался альтернативный подход к защите документов и этикеток подакцизных товаров. Для индивидуальной маркировки предлагается использовать уникальный идентификатор в виде линейного ШК, воспринимаемого обычным кассовым считывателем. Разработанные алгоритмы криптографических процедур создания и верификации многокомпонентного идентификатора предусматривают возможность как автономной, так и сетевой проверки его корректности. На основе использования результатов многократных сетевых проверок подобных уникальных идентификаторов обеспечивается возможность компьютерной реконструкции маршрута движения документов и партий товаров. Рассматривается возможность использования предлагаемого подхода для борьбы с неучитываемым

производством контрафактной продукции и преступлениями, совершаемыми с использованием фальсифицированных документов.