УДК 343.982/.983 МРНТИ 10.85.41

Ернар Нұрланұлы Бегалиев
Қазақстан Республикасы Бас прокуратурасының жанындағы Құқық қорғау органдарының академиясы, Нұр-Сұлтан қ., Қазақстан Республикасы, e-mail: ernar-begaliev@mail.ru

СТЕГАНОГРАФИЯЛЫҚ ТЕХНОЛОГИЯЛАРДЫ МАТЕРИАЛДЫҚ ОБЪЕКТІЛЕРДІҢ ЖЕКЕЛЕГЕН АЙЫРМАШЫЛЫҚТАРЫНЫҢ ҚҰРАМЫНА ЕНГІЗУ ПЕРСПЕКТИВАЛАРЫ ТУРАЛЫ

Аннотация. Автор әлемдік тәжірибе негізінде стеганографиялық технологияларды қолдану тәжірибесіне талдау жасайды. Дәстүрлі және сандық стеганографияны пайдаланудың түрлі салалары қарастырылды (IT - қауіпсіздік; өнеркәсіптік өндіріс және аудиовизуалды шығармаларды және бағдарламалық өнімдерді қорғау және т.б.). Зерттелетін әдістің күшті және әлсіз жақтарын қамтитын SWOT – талдау жүргізілді. Заңтану бойынша маманданған ғалымдардың, сондай-ақ осы мәселе бойынша өзге де ғылымдардың әртүрлі көзқарастары ұсынылады. Осы мақаланың басты өзегі – стеганография технологиясын қолдану шарттарын жедел, тергеу және сараптау практикасына енгізуге қатысты автордың тұжырымдары мен ұсыныстары болып табылады. Мақала тергеу әрекеттерін жүргізу тактикасы, қылмыстың жекелеген түрлерін (топтарын) тергеу әдістемесі мәселелеріне қызығушылық танытатын адамдарға, сондай-ақ оқырмандардың кең ауқымына арналған.

Түйінді сөздер: су белгісі, криптография, таңбалау, материалды объект, микрошрифт, стеганография.

Бегалиев Ернар Нурланович
Академия правоохранительных органов при Генеральной прокуратуре Республики Казахстан, г. Нур-Султан, Республика Казахстан, e-mail: ernar-begaliev@mail.ru

О ПЕРСПЕКТИВАХ ИНТЕГРИРОВАНИЯ СТЕГАНОГРАФИЧЕСКИХ ТЕХНОЛОГИЙ В СТРУКТУРУ ОТДЕЛЬНЫХ РАЗНОВИДНОСТЕЙ МАТЕРИАЛЬНЫХ ОБЪЕКТОВ

Аннотация. Автором приводится анализ практики применения стеганографических технологий на основе мирового опыта. Рассмотрены различные сферы использования традиционной и цифровой стеганографии (IT - безопасность; промышленное производство и защита аудиовизуальных произведений и программных продуктов и т.п.). Проведен SWOT – анализ, включающий в себя сильные и слабые стороны исследуемого метода. Предлагаются различные точки зрения ученых, специализирующихся на юриспруденции, а также иных науках по данной проблематике. Ключевым моментом данной статьи являются выводы и предложения автора касательно внедрения в оперативную, следственную и экспертную практику условий применения технологии стеганографии. Статья предназначена для лиц, интересующихся вопросами тактики производства следственных действий, методики расследования отдельных видов (групп) преступлений, а также для широкого круга читателей.

Ключевые слова: водяной знак, криптография, маркировка, материальный объект, микрошрифт, стеганография.

Begaliyev Ernar Nurlanovich
The Academy of Law Enforcement Agencies under the General Prosecutor's Office of the Republic of Kazakhstan, Nur-Sultan c., the Republic of Kazakhstan, e-mail: ernar-begaliev@mail.ru

ON THE PROSPECTS OF INTEGRATING STEGANOGRAPHIC TECHNOLOGIES INTO THE STRUCTURE OF INDIVIDUAL VARIETIES OF MATERIAL OBJECTS

Abstract. The author analyzes the practice of using steganographic technologies on the basis of world experience. Various spheres of traditional and digital steganography (IT - security; industrial

production and protection of audiovisual works and software products, etc.) are considered. The SWOT – analysis including strengths and weaknesses of the investigated method is carried out. Various points of view of scientists specializing in law and other Sciences on this issue are offered. The key point of this article is the author's conclusions and suggestions regarding the implementation of the operational, investigative and expert practice of the conditions of application of steganography technology.

The article is intended for people interested in tactics of investigative actions, methods of investigation of certain types (groups) of crimes, as well as for a wide range of readers.

Key words: watermark, cryptography, marking, material object, micro font, steganography.

Введение. В условиях стремительного развития цифровых технологий, мультимедийного оборудования, копировально-множительных средств, а также иных достижений научно-технического прогресса, повсеместно возрастает значение поиска и внедрения современных защитных инструментов, обеспечивающих безопасное обращение оригинальных материальных объектов. К таковым, на наш взгляд, в полной мере следует отнести метод стеганографии.

Цели и задачи. Целью настоящей статьи является определение условий и предметных рамок внедрения и использования стеганографической технологии в ходе раскрытия, расследования и предотвращения преступлений. Исходя из цели исследования, определены следующие задачи:

- провести анализ интеграционных процессов достижений научно-технического прогресса на предмет допустимости использования стеганографического метода в оперативной, следственной и экспертной практике;
- исследовать мировую практику применения стеганографии в различных сферах жизнедеятельности;
- внести предложения по интегрированию стеганографической технологии в практическую деятельность органов, осуществляющих раскрытие, расследование и предотвращение преступлений.

Методы исследования. Материалами исследования явились отдельные нормы уголовно-процессуального законодательства, регулирующие порядок производства некоторых следственных действий, научные публикации исследователей, а также материалы судебной и следственной практики по исследуемой теме. При написании статьи использовались нормативно-логический, формально-юридический и другие методы.

Результаты. Этимологически стеганография (греч. stegano – тайный + grapho - пишу) подразумевает способ скрытой передачи данных (текстовых или графических изображений), с целью дальнейшей идентификации материального объекта.

Принимая во внимание своеобразную специфичность области исследуемого вопроса, отмечаем существование достаточного количества этимологий, которые требуют детального анализа. Поэтому, считаем необходимым провести соотношение и разграничение существующих дефиниций, охватывающих рассматриваемую совокупность.

Так, под криптографией следует понимать высокотехнологичное направление, используемое при производстве документов, денежных знаков, ценных бумаг, бланков и пр., где тайнопись выступает в качестве защитной технологии от подделки вышеуказанных материальных объектов. В свою очередь, тайнопись понимается как техника исполнения символов и обозначений, направленная на ограниченное ознакомление третьими лицами с содержанием передаваемой информации. Если криптография выступает в качестве производного процесса, то тайнопись является конечным результатом высокотехнологичных процедур, причем, вне зависимости от ее разновидностей (водяной знак, микрошрифт и т.п.).

Процесс создания водяного знака предполагает технологию изготовления бумаги методом термического вдавливания печатных форм для создания изображений, формируемых за счет различия слоев целлюлозы. В настоящий момент наблюдается активное внедрение электронных (цифровых) водяных знаков в структуру мультимедийных материальных объектов.

Наконец, микрошрифтом является защитный элемент, выраженный в форме

непрерывной строки текста, уменьшенной до такой степени, что может быть прочитан только с помощью лупы.

Проводя структурные разграничения терминов «криптография» и «стеганография» мы склонны рассматривать данные процессы как общее и частное, где стеганография выступает подвидом криптографии, а последняя включает в себя достаточно объемный массив, содержащий непосредственно шифрование; разработку кодов; применяемое специальное оборудование; расходные материалы и многое др. Ключевым различием криптографии и стеганографии является цель нанесения соответствующих элементов на материальные объекты, где в криптографии отсутствует сама задача сокрытия факта передачи тайнописи (например, запрос получения кода либо наличие шифра). При стеганографической передаче зашифрованной информации, источником сведений может выступать любой материальный объект, представленный в определенных условиях места и времени. Поэтому, в структуре большинства существующих защитных элементов, включая описанные выше водяные знаки и микрошрифты, заложены криптографические, а не стеганографические, методы.

«Исследования и разработки в области стеганографии становятся все более популярными в современном информационном обществе наряду с широким использованием цифровых форматов мультимедиа и существующими проблемами управления цифровыми ресурсами и контроля использования прав собственности на компьютерные файлы. Вместе с тем, решение задачи сокрытия информации является важной проблематикой в условиях развитой инфраструктуры сетевого общения пользователей интернет - участников открытого и неконтролируемого взаимодействия в медиа пространстве» [1, с. 3].

В специальной литературе принято классифицировать стеганографию по следующим видам:

1. Традиционная (классическая).
2. Цифровая (мультимедийная).

Считаем необходимым отметить, что если традиционная стеганография имеет достаточно продолжительную историю своего существования, то цифровая является новеллой науки и техники.

В практике выявления, раскрытия, расследования и противодействия преступлений отмечено множество примеров эффективного использования традиционной стеганографии, среди которых следует выделить следующие виды деятельности:

а) как способ идентификации денежных знаков, переданных проверяемому лицу по делам о коррупционных правонарушениях (нанесение точек / проколов на полях банкнот);

б) как средство передачи невербальной информации, основанное на размещении условных сигналов и меток в структуре материальных объектов (при проведении проверочных следственных действий и оперативно-розыскных мероприятий);

в) как механизм защиты отдельных видов материальных объектов от подделки, заключающийся в их строгом соответствии и последовательном нахождении структурных элементов предметов, эмитентом которых выступают органы государственной власти (содержание цветовой гаммы и эскиз диплома, банкноты, паспорта и т.д.);

г) как элемент маркировки и контроля перемещения товарно-материальных ценностей по делам об экономической контрабанде (нанесение контрольных меток на продукцию, перемещаемую через государственную границу);

д) как средство персонализации факта изготовления либо владения конкретным материальным объектом (нанесение автографа, литеры или монограммы автором/правообладателем на объект интеллектуальной собственности, либо имеющего высокую стоимость).

На протяжении длительного периода времени, деятельность по передаче скрытой текстовой информации, в рамках традиционной стеганографии, успешно реализовывалась посредством применения симпатических чернил. В настоящий момент, внедрение технологии электронного документооборота, включающего проставление электронной цифровой подписи, по сути дела исключает необходимость применения пишущих приспособлений, в результате чего использование симпатических

чернил в современном документообороте видится нам малоэффективным.

Отдельными учеными предложен способ установления подлинности традиционных и электронных документов, заключающийся во «внедрении в них водяных знаков (для электронных документов – ЦВЗ). Причём внедряемые водяные знаки можно использовать как для доказательства подлинности документа, так и для встраивания в них определённой информации, например, для денежной купюры можно встроить серию и номер» [2, с.94; 3, с.2].

В отдельных случаях, традиционная стеганография может выступать в качестве объекта изобразительного искусства. К примеру, создание двух и более изображений, различных по стилю и содержанию, в структуре одного объекта требует от создателя произведения специальных навыков и умений.

Установление скрытой передачи информации при традиционной стеганографии, может являться предметом экспертного исследования в рамках технико-криминалистического исследования документов. Деятельность по обнаружению факта применения стеганографии именуется стегоанализом. В этой связи мы согласны с точкой зрения И. В. Нечты в том, что «задача стегоанализа состоит в обнаружении факта передачи секретного сообщения. Можно сказать, что стеганография и стегоанализ – два параллельно развивающихся направления науки» [4, с.4]. В европейской литературе проблемам применения стегоанализа посвящены труды Дж. Фридриха [5, с.67].

В качестве отличительной особенности цифровой стеганографии следует отметить передачу виртуальных данных со скрытым содержанием внутри одного объекта (файла). Данное направление может быть успешно реализовано только при помощи специальных программных устройств, при помощи которых исходное изображение может быть наложено на проецируемый ресурс. В зарубежной литературе рассматриваемая технология именуется как «Information Hiding» (Цифровая тайнопись) [6].

Мы в полной мере разделяем точку зрения Е. Ю. Митрофановой, которая указала на то, что «одним из востребованных подходов в этой области является применение технологий, базирующихся на использовании методов компьютерной стеганографии, позволяющих незаметно встраивать необходимые данные в любые информационные массивы и объекты цифрового контента (ОЦК) (файлы аудио и видеоданных, файлы текстовых форматов, неподвижные изображения и пр.). Указанные технологии широко используются при решении задач создания защищенной связи и передачи информации, цифровых водяных знаков, камуфлирования программного обеспечения и т.д.» [7, с.3]. Наиболее характерным преимуществом метода цифровой стеганографии является повышенный уровень конспирации, где установление самого факта его использования требует производства судебно-экспертных исследований.

В практике выявления, раскрытия, расследования и противодействия преступлений отмечены отдельные позитивные обстоятельства эффективного использования цифровой стеганографии, среди которых следует выделить следующие виды деятельности:

а) в качестве современной защитной технологии при легальном производстве мультимедийных аудиовизуальных произведений (аудио и видео продукции, клипы, ролики и т.д.);

б) в качестве современной защитной технологии при легальном изготовлении программных продуктов (программы, вирусы, софты, игры и т.п.);

в) как точное средство идентификации объекта в рамках судебно-экспертной деятельности;

г) в качестве средства персонификации виртуального контента конкретному правообладателю, включая установление непосредственного пользователя объектом / устройством.

В основу принципа цифровой стеганографии заложены 2 метода работы:

1. Установка меток на виртуальный продукт / используемое оборудование;

2. Нанесение цифровых водяных знаков.

Отмечая положительные свойства стеганографической технологии в процессе маркировки изображений в оптическом канале, М. В. Колесниковым справедливо отмечены следующие достоинства: «высокая степень устойчивости маркировки к имитации; возможность реализации для практически

любых устройств регистрации изображений без их существенных доработок» [8, с.1].

Нанесение идентификационных меток на виртуальный продукт является весьма эффективным средством защиты материальных объектов от подделки, так как позволяет осуществлять маркировку, включая размещение внутрикадровых стеганографических элементов. Более того, установка специальных приспособлений на мультимедийное оборудование (сканеров), решает задачи идентификации пользователей устройств и контента.

«Один из наиболее эффективных технических средств защиты мультимедийной информации заключается во встраивании в защищаемый объект невидимых меток – цифровых водяных знаков (ЦВЗ), которые позволяют тем или иным образом контролировать использование маркированного мультимедиа продукта. На практике наибольшее распространение получило маркирование цифровых изображений, что связано с их достаточно большой информационной емкостью» [9, с. 3].

Технология нанесения цифровых водяных знаков может также предполагать размещение специальных меток (знаков) с функцией отсылки данных, с целью проведения сравнительных экспресс исследований. Данная разработка активно внедрена в некоторых зарубежных государствах при изготовлении личных документов (паспортов, удостоверений личности). В ее основу заложено сопоставление текстов и изображений, благодаря фантомным аналогам.

Заключение.

В заключении сформулируем следующие выводы и предложения.

1. Принимая во внимание уникальные возможности реализации специальных функций (идентификация; установление подлинности; криминалистический учет и т.д.), при помощи метода стеганографии, считаем необходимым включить в технологические документы стандартизации (ГОСТы) производства отдельных разновидностей материальных объектов соответствующие требования по применению данной методики.

2. Следует активней использовать метод стеганографии, с целью установления источника происхождения материальных объектов, в интересах противодействия случаев экономической контрабанды, хищений, мошеннических действий, подделки документов, нарушений прав интеллектуальной собственности и иных правонарушений.

3. Склонны полагать абсолютно уместным и научно обоснованным процесс нанесения стеганографии в качестве одной из самостоятельных разновидностей защитной технологии материальных объектов от их подделки.

4. Считаем, что необходимо расширять ассортиментный ряд производимых материальных объектов, в которые может быть интегрирована стеганографическая информация.

Список использованных источников:

1. Кувшинов С.С. Методы и алгоритмы сокрытия больших объемов данных на основе стеганографии: автореф. дис. канд. тех. наук: 05.13.19. – СПб, 2010. - с. 19.
2. Сагайдак Д.А., Файзуллин Р.Т. Способ формирования цифрового водяного знака для физических и электронных документов // Компьютерная оптика, т. 38, №1. – 2014, – С. 94-104.
3. Bierbrauer J., Fridrich J. Constructing Good Covering Codes for Applications in Steganography // LNCS. Vol.4920 – Berlin, – 2008 – 22 p.
4. Нечта И.В. Разработка методов обеспечения безопасности использования информационных технологий, базирующихся на идеях стеганографии: автореф. дис. канд. тех. наук: 05.13.17. – Новосибирск, 2012. - 21 с.
5. Fridrich J. Feature – Based Stegoanalysis for JPEG Images and its Implications for Future Design of Steganographic Schemes // LNCS. Vol.3200 – Berlin, 2005 – 81 p.
6. Fabien A. P. Petitcolas, Ross J. Anderson and Marcus G. Kuhn. Information Hiding: A Survey // Proceedings of the IEEE. – San Jose, CA, 1999. – Vol. 87, №7. – 1078 p.
7. Митрофанова Е. Ю. Нейросетевые сжимающие преобразования данных и алгоритмы создания цифровых водяных знаков в объектах мультимедиа графических и звуковых форматов: автореф. дис. канд. тех. наук: 05.13.17. – Воронеж, - 2014. - 16 с.
8. Колесников М. В. Оптические методы и устройства для скрытой маркировки регистрируемых изображений: автореф. дис. канд. тех. наук: 05.11.07. – М., 2017. – 18 с.

9. Ван Цзянь. Исследование устойчивости цифровых водяных знаков – логотипов, внедряемых в статические изображения: автореф. дис. канд. тех. наук: 05.13.19. – СПб, 2010. – 20 с.

References:

1. Kuvshinov S. S. Metody i algoritmy sokrytiya bolshih objemov dannih na osnove steganografii: avtoref. dis. cand. tech. nauk: 05.13.19. – SPb, - s.19 (2010).

2. Sagaidak D. A., Faizullin R. T. Sposob formirovanija tsifrovogo vodjanogo znaka dlya fizicheskih i electronnih dokumentov // Kompyuternaya optika, t. 38, №1. s. 94-104 (2014).

3. Bierbrauer J., Fridrich J. Constructing Good Covering Codes for Applications in Steganography // LNCS. Vol.4920 – Berlin, 22 (2008).

4. Nechta I. V. Razrabotka metodov obespecheniya bezopasnosti ispolzovaniya informatsionnih technologiy, baziruyuschihsya na ideyah steganografii: avtoref. dis. cand. tech. nauk: 05.13.17. – Novosibirsk, - 21 (2012).

5. Fridrich J. Feature – Based Stegoanalysis for JPEG Images and its Implications for Future Design of Steganographic Schemes // LNCS. Vol.3200 – Berlin, 81 (2005).

6. Fabien A. P. Petitcolas, Ross J. Anderson and Marcus G. Kuhn. Information Hiding: A Survey // Proceedings of the IEEE. – San Jose, CA,– Vol. 87, №7. 1078 p. (1999).

7. Mitrofanova E. Yu. Neyroseteviye szhimauschiye preobrazovanija dannih i algoritmy sozdanija tsifrovih vodjanyh znakov v objektah multimediya graficheskih i zvukovih formatov: avtoref. dis. cand. tech. nauk: 05.13.17. – Voronezh, 16 (2014).

8. Kolesnikov M. V. Opticheskiye metody i ustroistva dlya skrytoi markirovki registriruemih izobrazheniy: avtoref. dis. cand. tech. nauk: 05.11.07. – M., 18(2017).

9. Van Tszyan. Issledovanije ustoichivosti tsifrovikh vodjanikh znakov – logotipov, vnedryaemykh v staticheskiye izobrazhenija: avtoref. dis. cand. tech. nauk: 05.13.19. – SPb, 20 (2010).