Введение Подсистемазащиты информации является важной составляющей системы безопасности предприятий [1]. В состав указанной подсистемы входят, в частности, различные криптографические средства. Используемые в них криптоалгоритмы подразделяются на симметричные, например AES, и асимметричные, например RSA [2]. Однако в ряде случаев разумной альтернативой криптографии является стеганография [3]. В работе [4] предложен базовый АЛГОРИТМ маскирования, применяемый для стегозащиты стилизованных бинарных изображений - описаний картографических сцен в терминах «объекты - координаты». Имена объектов и их координаты кодируются десятичными цифрами почтового алфавита. В результате бинаризации все 10 символов кода представляются двоичными матрицами-эталонами одинаковых размеров. Для них по АЛГОРИТМу случайно генерируется набор масок. Бинаризованные коды объектов и их координат погружаются по маскам в т.н. стегоконтейнеры, первоначально заполненные отрезками практически случайных последовательностей двоичных бит. При этом значения незамаскированных бит исходных матриц сохраняются. Тем самым осуществляется необходимая рандомизация. Известный набор масок является ключом распознавания. Оценка стойкости АЛГОРИТМа проводилась в работах [5, 6]. Рассматривались следующие виды атак: - атака путем полного перебора ключей; - атака с позиций точного знания некоторых типов объектов и их координат на карте; - ассоциации с картой местности; - атака на гамму. Была доказана вычислительная стойкость, связанная с невозможностью перебора ключей в приемлемое время. Вопросы помехоустойчивости. Для борьбы со случайными помехами и преднамеренными помехами дезинформации в работах [7, 8] были предложены: - модификация АЛГОРИТМА, заключающаяся в запрете использования в качестве дихотомизирующих битов эталонов, находящихся в узловых точках; - внедрение избыточности для обнаружения и возможной коррекции ошибок. При этом стойкость к атаке со знанием открытого текста не исследовалась. В этом случае аналитик имеет доступ не только к стеготекстам одного или нескольких сообщений, но и знает их открытые тексты. От него требуется найти ключ, который использовался для сокрытия этих сообщений. Постановка задачи Пусть в качестве открытого текста выступает последовательность 1 2 3 4 5 6 7 8 9 0, представленная в алфавите почтовых индексов. Противнику известен стеготекст данного сообщения, полученный с использованием АЛГОРИТМа двумерно-ассоциативного маскирования и процедуры рандомизации. Требуется оценить возможность нахождения секретного ключа (истинного набора масок), использованного при рандомизации. Поиск ключа осуществляется путем нахождения потенциальных битов дихотомизации, по которым формировался ключ (набор масок). Для этого проводится сравнение по каждому биту совокупности эталонов исходного сообщения и соответствующего ему стегосообщения. По каждому

совпадающему биту проводится дихотомизация исходного и стегосообщений на подмножества и далее процесс повторяется для полученных подмножеств. Результатом поиска будет являться множество ключей (наборов масок), по которым из исходного текста мог быть получен соответствующий стеготекст. Приведем алгоритм поиска. D0 и B0 содержат полное множество эталонов и соответствующих им рандомизированных объектов. 1. l = 0. l0 = 10. 2. A1 = (побитно). Эi - элементы множества Dl (эталоны). 3. A2 = (побитно). Oi - элементы множества Bl (рандомизированные объекты). 4. Провести побитное сравнение матриц A1 и A2. Определить количество совпадений kl при условии побитного равенства эталонов и соответствующих им рандоимзированных объектов по координатам совпадений. Сформировать список Cl+ 1 совпадающих координат. Если ll≠ 2, идти к п.5. Иначе - к п. 11 (при flagl= 1) либо к п. 16 (при flagl= 0). 5. kol1l : = 0, kol0l : = 0. l: = l + 1. 6. jl : = 1. 7. Для jl-координаты списка Cl сформировать два подмножества Dlи Bl из соответствующих элементов множества Dl-1и Bl-1, содержащих единицу по данной координате. Мощность сформированных подмножеств определяет величину ll. 8. Если Dlи Bl - единичные множества, идти к п.10. Иначе - к п.9. 9. flagl : = 1. Переход к п.2. 10. kol1l : = 1. 11. kol1l : = kl . 12. Для jl-координаты списка Cl сформировать два подмножества Dlи Bl из соответствующих элементов множества Dl-1и Bl-1, содержащих ноль по данной координате. Мощность сформированных подмножеств определяет величину ll. 13. Если Dlи Bl - единичные множества, идти к п.15. Иначе - к п.14. 14. flagl : = 0. Переход к п.2. 15. kol0l : = 1. 16. kol0l : = kl. 17. Если flagl-1 : = 1, то kol1l-1 : = kol1l-1 + kol1l · kol0l. Иначе kol0l-1 := kol0l-1 + kol1l · kol0l. 18. jl : = jl + 1. 19. Если jl 0, переход к п. 7 (при flagl = 0) либо к п. 13 (при flagl = 1).Иначе переход к п. 22. 22. Подсчет числа ключей считать законченным. Общее число ключей равно kol10 · kol00. 23. КОНЕЦ. Приведем пример работы представленного алгоритма для случая трех эталонов в множестве D0 в алфавите почтовых индексов (0, 1, 2). На рис. 1 сверху представлены двоичные матрицы для трех почтовых индексов 0, 1 и 2 размером 5×3. На этом же рис. снизу приведены те же эталоны, погруженные по маске в стегоконтейнер (т.е. рандомизированные объекты). Выделены местоположения возможных дихотомизирующих битов, совпадающих для соответствующих эталонов и их рандомизированных представлений. По первой координате эталон 0 противопоставляется эталонам 1 и 2. Определим дихотомизирующие биты этих двух эталонов. Их количество равно двум (см. рис. 2, а). По второй координате эталон 2 противопоставляется эталонам 0 и 1. Определим дихотомизирующие биты этих двух эталонов. Их количество равно четырем (см. рис. 2, б). Таким образом, общее число возможных ключей равно 6. Рис. 1 - Дихотомизирующие биты для трех эталонов а б Рис. 2 - Дихотомизирующие биты для двух эталонов Экспериментальные исследования Поиск ключей проводился для двух размеров эталонов m = 3 и m = 60 для трех случаев: базового

АЛГОРИТМА маскирования, модифицированного алгоритма и при внедрении избыточности. Результаты эксперимента представлены в табл. 1. Таблица 1 - Результаты эксперимента Размер эталонов m 3 60 Полное множество ключей 1013 1029 Базовый АЛГОРИТМ 103 1014 Модифицированный АЛГОРИТМ 103 1014 В табл. 1 приведены усредненные значения для 105 «прогонов» алгоритма поиска ключей для каждого из рассматриваемых случаев. Для всех рассмотренных случаев количество ключей при соответствующих значениях m одинаково, т.е. не зависит от модификации алгоритма и внедрения избыточности. Обсуждение Для m = 3 число полученных ключей составило всего 103. При этом по ранее проведенным исследованиям [6] полное множество ключей для этого случая - 1013. Таким образом, при m = 3 имеем потерю вычислительной стойкости. При m = 60 число полученных ключей составило 1014 при полном множестве ключей в 1029. Если принять время испытания одного ключа равным 1 секунде, то при условии одновременный работы 105 процессоров полный перебор займет около 30 лет. Полученные результаты свидетельствуют о возможности проведения потенциально успешной атаки со знанием открытого текста. Для сохранения вычислительной стойкости необходимо увеличение значения m. Однако увеличение m может привести к чрезмерному размеру ключа. Альтернативой является случай, когда изменение m не осуществляется, при этом, следуя общепринятой практике, проводится регулярная смена ключей с периодичностью один раз в сутки/неделю/месяц.