plexing. *Izvestiya Samarskogo nauchnogo centra Rossijskoj akademii nauk*, 2011, vol. 13, no. 6, pp. 48–51. (In Russ.)
5. Tsvetov V.P., Grafkin A.V., Lukanov A.S. Software stand for modeling digital channels of radio communication systems. *Aktualnye problemy radioelektroniki i telekommunikacij: materialy Vserossijskoj nauchno-tekhnicheskoj konferencii. Samara: OOO Artel,* 2023, *pp. 179–182.* (In Russ.)
6. Tsvetov V.P. et al. About one model of dynamic control of data flow in a radio channel. *Perspektivnye informacionnye tekhnologii: materialy Mezhdunarodnoj nauchno-tekhnicheskoj konferencii.* Samara, 2015, pp. 299–302. (In Russ.)
7. Tsvetov V.P. On one problem of decoding symbols using incomplete data in a radio channel. *Informacionnye tekhnologii i nanotekhnologii (ITNT-2017): materialy III Mezhdunarodnoj konferencii.* Samara, 2017, pp. 954–957. (In Russ.)
8. Tsvetov V.P. Using of interference for data protection in the radio channel. *Informacionnye tekhnologii i nanotekhnologii (ITNT-2020): materialy VI Mezhdunarodnoj konferencii.* Samara, 2020, pp. 255–260. (In Russ.)
9. Tsvetov V.P. Wireless channel noises and data protection. *CEUR Workshop Proceedings,* 2020, vol.2667, pp. 234–237.
10. Bakulin M.G. *OFDM technology: Textbook for Universities*. Moscow: Goryachaya liniya - Telekom, 2015, 360 p.

Reseived 12.10.2023

ЭЛЕКТРОМАГНИТНАЯ СОВМЕСТИМОСТЬ И БЕЗОПАСНОСТЬ ОБОРУДОВАНИЯ

УДК 621.372.552

ВЛИЯНИЕ ПРЕДВАРИТЕЛЬНОГО КРИПТОГРАФИЧЕСКОГО КОДИРОВАНИЯ СООБЩЕНИЯ НА ЕГО ОБНАРУЖИВАЕМОСТЬ В СТЕГАНОГРАФИЧЕСКИХ СИСТЕМАХ

Шамшаев М.Ю., Шакурский М.В.
Поволжский государственный университет телекоммуникаций и информатики, Самара, РФ
E-mail: maxsham2000@mail.ru, m.shakurskiy@gmail.com

Классическая задача стеганографии заключается в маскировке важного сообщения в покрывающем объекте, не представляющем интерес для злоумышленника. При этом внимание уделяется защите от обнаружения самого факта встраивания сообщения, так как в случае подозрения злоумышленником факта наличия скрытого сообщения в передаваемом информационном объекте злоумышленник может разрушить сообщение. Внимание же устойчивости к прочтению в стеганографии не уделяется, так как считается, что этот вопрос решается посредством предварительного криптографического шифрования сообщения. Однако, такое шифрование влияет на статистические параметры сообщения, что играет немаловажную роль при формировании стеганографической системы. Статья посвящена анализу влияния криптографического кодирования на потенциальную обнаруживаемость сообщения после стеганографической маскировки. Приводятся результаты исследования влияния криптографического кодирования на распределение значений передаваемой информации при использовании шифра «Кузнечик».

Ключевые слова: *стеганография, криптография, криптографическое кодирование, распределение значений*

Введение

В настоящее время вопрос безопасности передачи информации является одним из самых актуальных в области информационных технологий. Это связано как с переходом многих сфер человеческих и корпоративных взаимоотношений в области электронных систем передачи данных, так и с растущим уровнем киберпреступности. Очевидно, что системы защиты информации находятся в положении «отстающего», так как преступники постоянно находят новые пути обмана. С другой стороны, внедрение новых систем безопасности сковывается бюрократическим аппаратом в организациях. Тем не менее, постоянное развитие систем защиты информации значительно осложняет работу злоумышленников.

Одним из важных аспектов информационной безопасности является передача данных по открытым каналам связи, включающим в себя проводные и беспроводные сети, интернет и другие средства, где невозможно гарантировать отсутствие утечки передаваемой информации. Для решения задачи конфиденциальности передаваемых данных используется аппарат криптографии [1].

Задачей криптографического кодирования является обеспечение конфиденциальности передаваемой информации, то есть злоумышленник, зная о передаче информации, не имеет возможности ее дешифровки. Однако целостность передаваемой информации не гарантируется, так как в случае необходимости канал или сообщение могут быть разрушены. В случае, если злоумышленник способен разрушить сообщение, подозревая его ценность, криптографическое кодирование малоэффективно. Такая ситуация может возникнуть в случае тайной переписки, передачи сигналов управления беспилотными аппаратами и в других случаях. Тогда эффективным способом защиты является маскировка информации – стеганография. Здесь важно заметить, что стеганография не гарантирует целостность канала и сообщения. Они также могут быть разрушены. Речь идет о той грани, когда принимается решение о разрушении канала и сообщения. То есть, при перехвате информации злоумышленник не преследует цель разрушить канал и сообщение. Его задача - разрушить его только в случае передачи важного сообщения. Именно в этом свете маскировка важного сообщения в неважное способна обеспечить его доставку. Таким образом, ключевую роль играет не вопрос прочтения сообщения, а сам факт подозрения, что в передаваемой информации скрыто важное сообщение. Поэтому, в стеганографии вопрос политики злоумышленника, используемых им методов оценки передаваемой информации и набора возможных действий является открытым и требует дополнительных исследований.

При анализе стеганографических методов принимается определенная рабочая модель поведения злоумышленника. В соответствии с этой моделью производится исследование и анализ метода. При этом используется целый ряд допущений, которые на практике могут быть и некорректными.

Исследование, описанное в данной статье, позволяет уточнить модель стеганографической системы и проиллюстрировать совместное использование стеганографического и криптографического кодирования.

В научной литературе [1; 2] указывается, что при стеганографической маскировке сообщения, защита от прочтения решается предварительным криптографическим шифрованием. Например, современные блочные шифры обладают достаточной устойчивостью к взлому и высокой скоростью шифрования. Однако, важным вопросом стеганографии является характер шифруемого сообщения. Учитывая объем передаваемых данных, акцент в стеганографическом анализе делается на статистических методах оценки информации, передаваемой по открытому каналу связи. При анализе методов стеганографии мало внимания уделяется статистическому характеру сообщения. Так часть встраиваемого сообщения может состоять из последовательности только нулей или только единиц, что может оказать значительное влияние на статистические характеристики стеганографической системы (заполненного стеганографического контейнера). Предварительное криптографическое шифрование оказывает определенное влияние на статистические характеристики сообщения. При этом многообразие различных вариантов шифрования может оказывать различное влияние на параметры встраиваемого сообщения. Таким образом, предварительное криптографическое шифрование позволяет не только обезопасить встраиваемое сообщение от прочтения, но и уточнить статистическую модель встраиваемого сообщения, что, в свою очередь, позволит уточнить потенциальную полезную нагрузку стеганографической системы.

В статье взят для анализа шифр «Кузнечик». Криптографический шифр «Кузнечик» использует блочное шифрование с длиной блока 128 бит и ключом длиной 256 бит. Шифр работает в режиме ECB (electronic code book) или в режиме простой замены. В процессе шифрования используется матрица 8x8, которая состоит из 64 байтов, и представляет собой расширенный вектор [3].

Процесс шифрования происходит в 10 раундов, в каждом из которых используется 8 нелинейных преобразований и 1 линейное преобразование. Нелинейные преобразования основаны на заменах байтов и перестановках битов, а линейное преобразование основано на умножении матрицы на столбец данных [4].

Данный шифр утвержден в качестве стандарта в ГОСТ Р 34.12-2015 «Информационная технология. Криптографическая защита информации. Блочные шифры» приказом от 19 июня 2015 года № 749-ст. Стандарт вступил в действие с 1 января 2016 года. Шифр разработан Центром защиты информации и специальной связи ФСБ России с участием АО «Информационные технологии и коммуникационные системы» [5–10].

Моделирование криптографического шифрования

Компьютерное моделирование шифрования выполнено на языке Python. В качестве сообщения выбраны три набора с различным распределением значений: с одинаковым количеством нулей и единиц, с доминирующим количеством нулей и с доминирующим количеством единиц. Это позволило оценить влияние шифрования на распределение значений в зашифрованных сообщениях. Сами значения подбирались генератором псевдослучайных чисел.

Для проведения эксперимента была создана программа генерации исходного сообщения в двоичной системе счисления, которая формирует сообщение длинной 1024 символа с указанным распределением нулей и единиц. Также программа переводит полученное число из двоичной системы счисления в шестнадцатеричную. Код программы приведен ниже:

```
import random
# Генерация случайного сообщения
message_length = 1024
zero_percent = 95 #  Процент нулей
message = “”.join (
    “0” if random.randrange (100) < zero_percent else “1”
    for _ in range (message_length)
)
print («Сообщение в двоичном виде:», message)
# Перевод двоичного сообщения в шестнадцатеричное
hex_message = hex (int(message, 2))[2:]
print («Сообщение в шестнадцатеричном виде:», hex_message.upper ())
```

Выходные данные программы генерации сообщения:

Сообщение в 16-ричном виде: 93A038991EEF74F256F19F80639B4371EDCF1B7D0176A4865A2FF7FF209A41F240C023F8D3501178D8D6B7B7266CFEF78AAF76D1D4461BDAF773A56EAED11C84878EC935B53C3151BE33C576C44B215623C06FFDEC36BCF3CCC0BEC8FB08F4CADBC2843CC4F85AD12A5B7318EE57A77443E2C0991DE3471BF156415F651E3CD9.

Следующим шагом полученное сообщение в шестнадцатеричном виде шифруется при помощи криптографического шифра «Кузнечик». В результате шифрования получено сообщение, представленное ниже.

Зашифрованное сообщение в 16-ричном виде: D206700720EAD67902EAACA5DE855A8585512E8D93CEE3067A4D6CDCF799B2E79AF8B3B4FC82F13A0D6B07A979A8D9A3A8BF70A30BEA66C31C95B9B6245C469EB89B6E19078AAFC3B8B0D13D87BF4D5F9D30EF62CBF512FFADA0D17BA473735E4C49783FDS201FCEES8ED91B082C72S4E261C20B89BBB4D1A49C5746S7D66D85

Проведем анализ распределения значений в зашифрованном сообщении. Для этого воспользуемся встроенным аппаратом построения гистограмм. Код программы построения гистограмм приведен ниже:

```
import matplotlib.pyplot as plt
def count_zeroes_ones (message):
    zeroes = message.count (‘0’)
    ones = message.count (‘1’)
    return zeroes, ones
def main ():
    message1 = input («Введите исходное сообщение: «)
    message2 = input («Введите зашифрованное сообщение: «)
    zeroes1, ones1 = count_zeroes_ones (message1)
    zeroes2, ones2 = count_zeroes_ones (message2)
    labels = [‘Нули’, ‘Единицы’]
    message1_data = [zeroes1, ones1]
    message2_data = [zeroes2, ones2]
    x = range (len(labels))
    fig, ax = plt.subplots ()
    ax.bar (x, message1_data, width=0.3, label=’Исходное сообщение’)
    ax.bar ([x_elem + 0.3 for x_elem in x], message2_data, width=0.3, label=’Зашифрованное сообщение’)
    ax.set_ylabel (‘Количество’)
    ax.set_xlabel (‘Данные’)
    ax.set_title (‘Распределение нулей и единиц’)
    ax.set_xticks ([x_elem + 0.15 for x_elem in x])
    ax.set_xticklabels (labels)
    ax.legend ()
ax.grid (True)
ax.set_ylim ([0, max(max(message1_data), max (message2_data))+1])
plt.show ()
if __name__ == ‘__main__’:
main ()
```

Из проведенных экспериментов для анализа выбраны три с различным соотношением количества нулей и единиц в шифруемом сообщении.

Эксперимент №1: 50% нулей и 50% единиц. Результат моделирования приведен в виде диаграммы на рисунке 1.

Эксперимент №2: 5% нулей и 95% единиц. Результат моделирования приведен в виде диаграммы на рисунке 2.

Эксперимент №3: 95% нулей и 5% единиц. Результат моделирования приведен в виде диаграммы на рисунке 3.

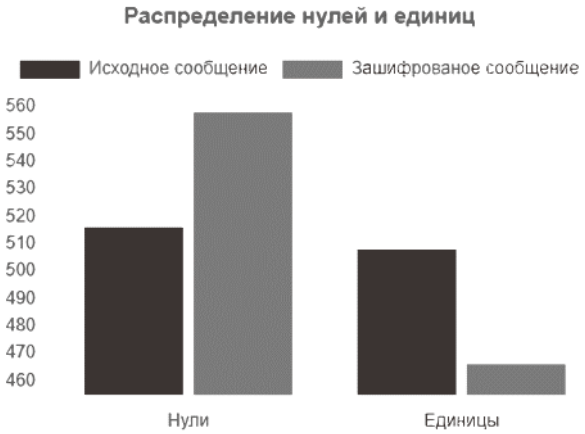

Рисунок 1. Результат моделирования при 50% логических нулей и 50% логических единиц

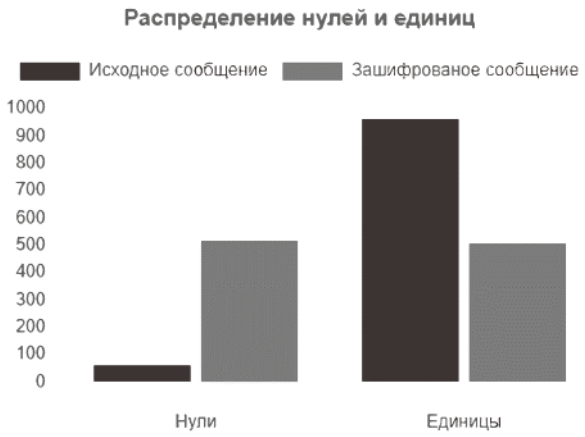

Рисунок 2. Результат моделирования при 5% логических нулей и 95% логических единиц

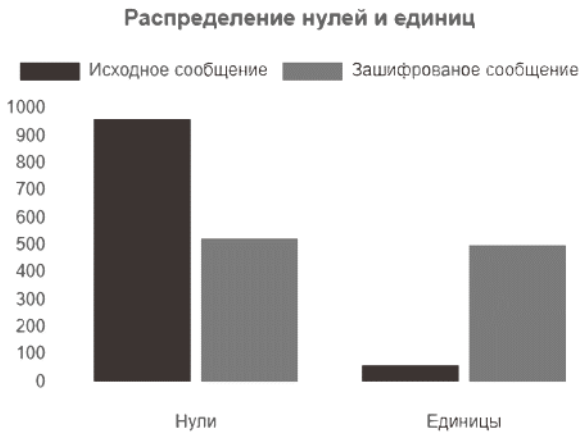

Рисунок 3. Результат моделирования при 95% логических нулей и 5% логических единиц

Видно, что в результате шифрования распределение значений становится близким к равномерному. Данный результат говорит в пользу использования блочных шифров на основе сети Фейстеля, так как позволяет построить модель стеганографической системы, в которой сообщение всегда имеет распределение близкое к равномерному.

Анализ эксперимента и заключение

Полученный в работе результат имеет важное значение, так как позволяет определить статистические характеристики сообщения. Например, если допустить, что сообщение предварительно криптографически зашифровано, то при проектировании и исследовании стеганографических систем можно считать, что распределение значений сообщения близко к равномерному.

Важно отметить, что не все шифры оказывают аналогичное воздействие на распределение значений в сообщении, что требует развития исследований. Полученное равномерное распределение значений сообщения не является однозначным достоинством. С одной стороны, совместно с использованием маскировки в наименьшем битном слое покрывающего объекта, можно считать такое распределение достоинством, с другой стороны только по отношению к покрывающим объектам, где наименьший битный слой обладает равномерным распределением. Это встречается не так уж часто. Более того, в работах [6–9] показано, что равномерное распределение в наименьшем битном слое может рассматриваться как индикатор наличия скрытого сообщения, которое может быть легко обнаружено на основе NIST-тестов.

Таким образом, использование блочных шифров позволяет сделать распределение встраиваемых сообщений близким к равномерному, что позволит более точно определить предел полезной нагрузки при формировании стегосистемы на основе известных методов и обеспечить конфиденциальность скрытой информации. Однако в системах реального времени использование блочных шифров для предварительного шифрования может привести к потенциальной уязвимости стегосистемы, так как статистический характер покрывающего объекта случаен и не может быть предварительно проанализирован [10].

Литература

1. Таранников Ю. Зачем в криптографии используется кодирование? URL: https://postnauka.ru/faq/85941 (дата обращения: 06.05.2023).
2. Агурьянов И. Виды и способы криптографических преобразований. URL: https://www.securitylab.ru/blog/personal/aguryanov/29980.php (дата обращения: 06.05.2023).
3. Криптографический алгоритм «Кузнечик»: просто о сложном. URL: https://habr.com/ru/articles/459004/ (дата обращения: 06.05.2023).

4. Дроботун Е. Работаем с алгоритмом блочного шифрования «Кузнечик» из ГОСТ 34.12-2015. URL: https://xakep.ru/2017/02/02/working-with-grasshopper/ (дата обращения: 06.05.2023).
5. Шишкин В. ГОСТ Р 34.12–2015: чего ожидать от нового стандарта? URL: https://lib.itsec.ru/articles2/crypto/gost-r-chego-ozhidat-ot-novogo-standarta (дата обращения: 06.05.2023).
6. Гистограммы и графики распределения в Python. URL: https://itnan.ru/post.php?c=1&p=683738 (дата обращения: 06.05.2023).
7. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. 2-е изд. М.: СОЛОН-Пресс, 2021. 262 с.
8. Обзор методов статистического анализа данных. URL: http://statlab.kubsu.ru/node/4 (дата обращения: 06.05.2023).
9. Шифр «Кузнечик» (ГОСТ Р 34.12-2015) и режимы работы блочных шифров (ГОСТ Р 34.13-2015). URL: https://studme.org/239569/informatika/shifr_kuznechik_gost_3412_2015_rezhimy_raboty_blochnyh_shifrov_gost_3413_2015 (дата обращения: 06.05.2023).
10. Караулова О.А., Шакурский М.В. Особенности оценки стеганографических систем с точки зрения стеганографического анализа // Ассоциация выпускников и сотрудников ВВИА имени профессора Н.Е. Жуковского: материалы XIX Международной научно-практической конференции, 2022. С. 66–70.

Получено 05.09.2023

Шамшаев Максим Юрьевич, магистрант кафедры информационной безопасности (ИБ) Поволжского государственного университета телекоммуникаций и информатики (ПГУТИ). 443010, Российская Федерация, г. Самара, ул. Л.Толстого, 23. Тел. +7 960 817-26-89. E-mail: maxsham2000@mail.ru

Шакурский Максим Викторович, д.т.н., заведующий кафедрой ИБ ПГУТИ. 443010, Российская Федерация, г. Самара, ул. Л.Толстого, 23. Тел. +7 (927) 772-98-73. E-mail: m.shakurskiy@gmail.com

THE IMPACT OF PRE-CRYPTOGRAPHIC CODING MESSAGES ON ITS DETECTABILITY IN STEGANOGRAPHIC SYSTEMS

Shamshaev M.Yu., Shakurskiy M.V.
Povolzhskiy State University of Telecommunications and Informatics, Samara, Russian Federation
E-mail: maxsham2000@mail.ru, m.shakurskiy@gmail.com

The usual problem of steganography is to mask an important message in a covering object that is of no interest to the attacker. In this case, attention is paid to protection from detection of the very fact of the message embedding a, since if an attacker suspects the presence of a hidden message in the transmitted information object, he can destroy the message. By the way no attention is paid to reading tolerance in steganography, since it is believed that this issue is solved by preliminary crypto-graphic encryption of the message. However, such encryption affects statistical parameters of the message, which plays an important role in the steganographic system formation. The article is devoted to the analysis of the influence of cryptographic coding on the potential detectability of the message after steganographic masking. The results of the study on the influence of crypto-graphic coding on the transmitted data distribution values when using the «Kuznyechik» cipher are presented.

Keywords: *cryptography, cipher, cryptographic coding, python, value distribution*

DOI: 10.18469/ikt.2023.21.2.12

Shamshaev Maxim Yurievich, Povolzhskiy State University of Telecommunications and Informatics, 23, L. Tolstoy Street, Samara, 443010, Russian Federation; Master's Degree Student of Information Security Department. Tel. +7 960 817-26-89. Email: maxsham2000@mail.ru

Shakurskiy Maxim Viktorovich, Povolzhskiy State University of Telecommunications and Informatics, 23, L. Tolstoy Street, Samara, 443010, Russian Federation; Head of Information Security Department, Doctor of Technical Sciences. Tel. +7 927 772-98-73. Email: m.shakurskiy@gmail.com

References

1. Tarannikov Yu. Why is coding used in cryptography? URL: https://postnauka.ru/faq/85941 (accessed: 05.06.2023). (In Russ.)

2. Aguryanov I. Types and methods of cryptographic transformations. URL: https://www.securitylab.ru/blog/personal/aguryanov/29980.php (accessed: 05.06.2023). (In Russ.)
3. Cryptographic algorithm «Grasshopper»: just about the complex. URL: https://habr.com/ru/articles/459004/ (accessed: 05.06.2023). (in Russ.)
4. Drobotun E. We work with the block cipher algorithm «Grasshopper» from GOST 34.12-2015. URL: https://xakep.ru/2017/02/02/working-with-grasshopper/ (accessed: 05.06.2023). (In Russ.)
5. Shishkin V. GOST R 34.12–2015: what to expect from the new standard? URL: https://lib.itsec.ru/articles2/crypto/gost-r-chego-ozhidat-ot-novogo-standardta (accessed: 05.06.2023). (In Russ.)
6. Histograms and distribution plots in Python. URL: https://itnan.ru/post.php?c=1&p=683738 (accessed: 05.06.2023). (In Russ.)
7. Gribunin, V. G., Okov, I. N., Turintsev, I. V. *Digital steganography*. 2nd Ed. Moscow: SOLON-Press, 2021, 262 p. (In Russ.)
8. Overview of statistical data analysis methods. URL: http://statlab.kubsu.ru/node/4 (accessed: 05.06.2023). (In Russ.)
9. Cipher «Grasshopper» (GOST R 34.12-2015) and operating modes of block ciphers (GOST R 34.13-2015). URL: https://studme.org/239569/informatika/shifr_kuznechik_gost_3412_2015_rezhimy_raboty_blochnyh_shifrov_gost_3413_2015 (date of access: 05/06/2023). (In Russ.)
10. Karaulova O. A., Shakursky M. V. Peculiarities of evaluating steganographic systems from the point of view of steganographic analysis. *Association of graduates and employees of VVIA named after Professor N.E. Zhukovsky: materialy XIX International Scientific and Practical conferences*, 2022, pp. 66–70. (In Russ.)

Received 05.09.2023

УПРАВЛЕНИЕ И ПОДГОТОВКА КАДРОВ ДЛЯ ОТРАСЛИ ТЕЛЕКОММУНИКАЦИЙ

УДК 004.04

СКВОЗНЫЕ ТЕХНОЛОГИИ В ОБРАЗОВАТЕЛЬНОЙ СИСТЕМЕ ВУЗА

Малина А.Б.[1,2], Тарутин Н.А.[1]
[1]Самарский государственный технический университет, Самара, РФ
[2]Самарский государственный социально-педагогический университет, Самара, РФ
E-mail: kuzdavletova_ab@mail.ru, nikitarutin@mail.ru

В данной статье авторы рассматривают инновационные подходы к внедрению сквозных технологий в сферу образования. Сквозные технологии – это принципиально новые технологические решения, которые проникают во всех стадиях образовательного процесса, объединяя учебные программы, методы обучения и оценку результатов воедино. Целью данной статьи является изучение сквозных технологий с целью повышения эффективности образования, улучшения доступности образовательных ресурсов, а также развития критического мышления и творческих навыков учащихся. В статье проведен анализ существующих сквозных технологий, и выявлены наиболее перспективные подходы для внедрения в образовательный процесс. Разработаны практические инструменты и методики, основанные на использовании сквозных технологий, которые могут быть применены в учебных заведениях различного уровня. В рамках исследования авторы также уделяют внимание аспекту подготовки педагогического состава к использованию сквозных технологий. Отмечается, что интеграция данных технологий помимо технической требует и педагогической подготовки.

Ключевые слова: *сквозные технологии, цифровизация образования, искусственный интеллект, обучение, качество образования*

Введение

Новые технологические достижения играют важную роль в непрерывном развитии современного образовательного пространства. Благодаря появлению информационных и коммуникационных технологий стало возможным переосмысле-