УДК 53.06

ИССЛЕДОВАНИЕ УСТОЙЧИВОСТИ СИСТЕМЫ ПЕРЕДАЧИ ДАННЫХ НА ОСНОВЕ ФАНТОМНОЙ ВИЗУАЛИЗАЦИИ И МЕТОДА МНОЖЕСТВЕННОГО ДОСТУПА С КОДОВЫМ РАЗДЕЛЕНИЕМ К ОСНОВНЫМ ВИДАМ АТАК

Мочалов М.А. (ИТМО)**, Старцева А.М.** (ИТМО)**, Шумигай В.С.** (ИТМО)**.**
Научный руководитель – доктор физико-математических наук, доцент Цыпкин А.Н. (ИТМО)

Введение. В настоящее время для передачи данных оптическими методами активно используется методика вычислительной фантомной визуализации (с англ. GI – ghost imaging), в рамках которой объект наблюдения освещается набором заданных оптических полей, формирование которых обеспечивается пространственным модулятором света. Для задач передачи данных данная методика применяется ввиду наличия двух переменных для кодирования – интегральные интенсивности прошедшего через объект излучения и набора оптических полей, а также из-за возможности работы в системах с большими шумами. Однако, чтобы процесс передачи данных был защищенным, необходимо закодировать имеющиеся данные. Так, на сегодняшний день существует множество способов кодирования данных, среди которых выделяется метод множественного доступа с кодовым разделением (с англ. CDMA – code division multiple access), так как при его использовании появляется возможности работы с несколькими пользователями. Ранее была представлена система передачи данных на основе временной GI и метода CDMA, однако основным ее недостатком была излишняя загруженность закрытого канала передачи данных, который использовался для передачи паттернов освещения [1]. В Университете ИТМО была предложена другая модель передачи данных на основе пространственной GI и метода CDMA [2]. Эта модель имеет большие перспективы в прикладном применении, так как она решает основную проблему своего предшественника – загруженность закрытого канала связи. Однако до сих пор не было проведено исследований по оценке безопасности процесса передачи данных.

Основная часть. Для анализа безопасности этой системы используются три ключевые атаки: атака на зашифрованный текст, атака с выбранным текстом и дифференциальная атака. Эти атаки были выбраны, так как они способны выявить уязвимости в системе и оценить ее устойчивость к различным видам атак. Это стандартный подход при анализе подобных систем для обеспечения их надежности и безопасности [1, 3]. Ниже представлено описание и применение каждой атаки к используемой системе.

1) Атака на зашифрованный текст — это тип криптографической атаки, при которой злоумышленник имеет доступ только к зашифрованному тексту, но не имеет информации о ключе шифрования, открытом тексте или структуре шифрования. Основная цель такой атаки заключается в восстановлении открытого текста или ключа шифрования. Для оценки устойчивости системы к этой атаке проводился анализ статистический характеристик зашифрованного текста.

2) Атака с выбранным текстом — это тип атаки, при которой злоумышленник имеет возможность выбирать исходные (открытые) тексты и получать соответствующие зашифрованные тексты. Это является более мощной атакой по сравнению с атакой на зашифрованный текст, так как злоумышленник имеет контроль над выбранными данными. Для проверки системы рассматривался частный случай, который является самым «простым» для злоумышленника, потому что в нем используется не большой секретный ключ и всего 3 получателя.

3) Дифференциальная атака – атака с использованием выбранного текста при взломе систем шифрования. В этом способе злоумышленнику необходимо изменять небольшое количество входных данных и анализировать, как это влияет на

зашифрованный результат для раскрытия ключа. Для оценки безопасности статистически анализировалась связь между открытым и зашифрованным текстом.

Выводы. Была проверена устойчивость компьютерной модели системы передачи данных на основе фантомной визуализации и множественного доступа с кодовым разделением к основным видам атак. Данный анализ подчеркивает прочность и эффективность отечественной системы передачи данных в защите от кибератак, как на открытый, так и на зашифрованный текст.

Список использованных источников:

1. Kang Y, Zhang L., Ye H., Zhao M., Saima K., Chunyan B., Zhang D. One-to-many optical information encryption transmission method based on temporal ghost imaging and code division multiple access // Photon. Res. –2019. –V.7 –P.1370-1380
2. Лейбов Л.С., Цыпкин А.Н., XI Конгресс молодых учёных. 237-240, (2022).Muniraj, I., Sheridan J.T. Optical Encryption and Decryption –SPIE PRESS BOOK, 2019. –48 p.
3. Kang Y, Zhang L., Ye H., Zhao M., Saima K., Zhang D. Camouflaged Optical Encryption Based on Compressive Ghost Imaging // Optics and Lasers in Engineering –2020. –V.134.