ДОСЛІДЖЕННЯ ТЕХНОЛОГІЇ ОПИСУ ЛІНІЙНИХ І НЕЛІНІЙНИХ КРИПТОГРАФІЧНИХПЕРЕТВОРЕНЬ ОПЕРАЦІЙ

Мельник О.Г., Мельник Р.П.
Черкаський інститут пожежної безпеки імені Героїв Чорнобиля НУЦЗ України, Черкаси, Україна

Розширення спектру операцій, на основі яких будуються криптографічні алгоритми, є одним із перспективних шляхів удосконалення існуючих криптографічних систем захисту інформації та розробки нових криптографічних алгоритмів [1]. Тому задача синтезу нових операцій криптографічного перетворення інформації є надзвичайно актуальною.

Метою доповіді є представлення результатів дослідження запропонованої технології опису залежності розрахунку кількості операцій криптографічного перетворення, що базується на рекурентному поєднанні потужностей множин операцій меншої розрядності та елементарних функцій[2].

В доповіді наводяться проміжнірезультати досліджень запропонованої технології опису лінійних і нелінійних криптографічних перетворень, що за попередніми висновками, є коректною і математично описує процес побудови множин нових операцій.

Базуючись на результатах проведеного дослідження, можна вважати, що розробка єдиної технології синтезу та дослідження як лінійних, так і нелінійних операцій криптографічного перетворення інформації є перспективною та цілком можливою. Запропонований підхід дозволяє розраховувати кількість операцій криптографічного перетворення інформації та будувати самі операції шляхом поєднання відомих операцій криптоперетворення та елементарних функцій більшої розрядності [3].

Даний підхід створює передумови для розробки єдиної технології опису та синтезу як лінійних, так і нелінійних операцій криптоперетворення.

Список літератури

1. Криптографічне кодування: обробка та захист інформації / під ред. В.М. Рудницького. Харків: ТОВ «ДІСА ПЛЮС», 2018. 139 с.
2. Рудницкий В. Н., Пивнева С. В., Бабенко В. Г., Миронец И. В., Дмитришин А. В., Барышев Ю. В. Криптографическое кодирование: методы и средства реализации: монография. Тольятти, 2013. 196 с.
3. Рудницкий В. Н., Мельник Р. П., Мельник О. Г. Повышение быстродействия систем защиты информации. Чрезвычайные ситуации: теория, практика, инновации «ЧС – 2012»: сборник материалов международной научно-практической конференции. Гомель : ГГТУ им. П.О. Сухого, 2012. С. 224.

ПРОБЛЕМИ ПРОТИДІЇ ТЕКСТОВІЙ ПРОПАГАНДІ

Тарасенко Я.В.
Черкаський державний технологічний університет, Черкаси, Україна

Процеси глобалізації суспільства забезпечують безперешкодне поширення інформації, в тому числі і маніпулятивного характеру. В той же час, необхідність забезпечувати свободу слова унеможливлює обмеження доступу громадян до потенційно-шкідливих ЗМІ. Це зумовлює необхідність вирішення проблеми цільового виявлення та протидії текстовійпропаганді.І, хоча засобами інформаційно-психологічного протиборства можуть бути Інтернет-ресурси чи друковані ЗМІ [1], проте головним носієм пропаганди залишається текст. Однак, існують певні проблеми протидії текстовій пропаганді, які методи нейро-лінгвістичного програмування не в змозі вирішитиу зв'язку з непередбачуваними результатами, які не гарантують високого рівня безпеки [2]. До таких проблем відносяться питання пов'язані з визначенням притаманності текстових морфологічно-синтаксичних конструкцій пропагандисту.

Метою доповіді є побудова моделі оцінки притаманності складників морфологічно-синтаксичної категорії психолінгвістичного портрету пропагандисту, що дозволить підвищити точність визначення семантичної частки.

У доповіді наводяться результати дослідження типовості використання відповідних синонімічних груп складників морфологічно-синтаксичної категорії маніпулятивного тексту та порівняння результатів зі звичайними текстами на таку ж тематику за умов їх написання однією та різнимиособами. Отримані дані виявляють закономірності у використанні морфологічно-синтаксичних засобів, що допомагає вирішити проблему протидії текстовій пропаганді. Структурна адаптація синтаксичної конструкції відповідно до співрозмовника [3] використовується і в маніпулятивних цілях, а отже виявлення її слідів та причин дасть змогу підвищити ефективність протидії пропаганді за рахунок високої точності визначення психолінгвістичних особливостей, що дозволить покращити підхід кореляції морфологічно синтаксичної категорії з семантичною категорією психолінгвістичного портрету пропагандиста.

Список літератури

1. Грищук Р. В., Канкін І. О., Охрімчук В. В. Технологічні аспекти інформаційного протиборства на сучасному етапі. *Захист інформації*. 2015. Т. 17, № 1. С. 81–86.
2. Тарасенко Я. В. Використання принципів квантової лінгвістики в інформаційному протиборстві. Безпека інформації. 2019. Т. 25, № 2. С. 96-103. DOI: https://doi.org/10.18372/2225-5036.25.13671
3. Heyselaar E., Hagoort P., Segaert K. How social opinion influences syntactic processing – An investigation using virtual reality. *PLoS ONE*. 2017. № 12 (4). URL:https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0174405(дата звернення: 08.10.2019). DOI: https://doi.org/10.1371/journal.pone.0174405