УДК 004.056.55

А.В. ГАЛЬЧЕНКО, С.В. ЧОПОРОВ
Запорізький національний університет

КОДУВАННЯ ДАНИХ В АЛГОРИТМАХ ЗАПЕРЕЧУВАНОГО ШИФРУВАННЯ

Дане дослідження проведене авторами для перевірки гіпотези щодо можливості збільшення швидкості роботи алгоритмів заперечуваного шифрування, без внесення змін безпосередньо у вихідні алгоритми. Вказане дослідження є актуальним, оскільки алгоритми заперечуваного шифрування мають дієві схеми для захисту інформації та її користувачів. Однак структура вказаних алгоритмів складна та зосереджена, що досить сильно впливає на швидкість їх роботи та робить неможливим практичне застосування алгоритмів заперечуваного шифрування даних для вирішення завдань із захисту інформації. Основною метою дослідження є огляд алгоритмів кодування інформації, які дозволяють маніпулювати розміром даних шляхом зміни їх форми, але не інформаційної складової. Використання алгоритмів кодування в теорії повинне суттєво зменшити розмір даних, які обробляються алгоритмами заперечуваного шифрування. Вказаний підхід повинен забезпечити пропорційне зростання швидкодії алгоритмів заперечуваного шифрування та створити умови для їх практичного використання в подальшому. В цій роботі виконано огляд ефективних алгоритмів кодування даних і їх застосування в процедурах обробки інформації алгоритмів заперечуваного шифрування. Під час досліджень було розглянуто два алгоритми. Перший з них є базовою моделлю для блочного шифрування даних з використанням механізмів заперечуваного шифрування, недоліки безпеки в його роботі були виявлені та досліджені. Інший алгоритм побудований на основі імплементації ефективних алгоритмів кодування інформації в підсистему обробки даних базової моделі. Ефективність роботи обох алгоритмів була перевірена на реальних файлах з публічною та секретною інформацією. Дослідження проводилося на стендовому апаратному та програмному забезпеченні, яке імітує робоче місце користувача. Результати експериментів демонструють появу приросту в швидкості виконання вихідного алгоритму заперечуваного шифрування даних за рахунок зменшення розміру вхідних даних. Додатково було перевірено залежність отриманих результатів від ключів шифрування різного розміру. Отримані результати були порівняні з результатами досліджень інших авторів. Враховуючи результати експериментів гіпотеза авторів була підтверджена, оскільки кодування даних вхідних даних призвело до значного скорочення розміру вхідних даних та відповідного приросту швидкості їх виконання.

Ключові слова: заперечуване шифрування; захист інформації; конфіденційні дані; компресія даних; несанкціонований доступ; примушування; продуктивність; стиснення даних; шифр.

A.V. HALCHENKO, S.V. CHOPOROV
Zaporizhia National University

THE DATA ENCODING IN DENIABLE ENCRYPTION ALGORITHMS

The hypothesis of the deniable encryption algorithms productivity increasing without the original algorithms transformation possibility has been investigated in this article. The algorithms of deniable encryption is relevant because of effective protection schemes of information and its users. These algorithms have the complex and concentrated structure. It makes impossible their practical applying. Its productivity is affected by them. That's why

10.32782/KNTU2618-0340/2020.3.2-1.6

deniable encryption algorithms are not applied for practical using. The encoding information algorithms reviewing and its investigation are main objectives of the article. They allow to transform the information, not its value. The deniable encryption algorithms input data is reduced by the encoding algorithms. The deniable encryption algorithms proportional productivity increasing and their practical applying are provided. The effective encoding algorithms and their applications are overviewed and applied to deniable encryption algorithms in this manuscript. Two algorithms have been investigated. The first scheme is based on the deniable encryption mechanisms. Its security bugs have been identified and investigated. Another algorithm is based on the efficient encoding algorithms. They are implemented to the basic data processing subsystem. Both of the algorithms' efficiency has been investigated by the real public and secret information files using. The proposed data processing schemes are investigated by the user's workplace simulating. The original deniable encryption algorithm productivity increasing has been reached by the reduced data size. Also, the encryption keys difference and its dependence have been tested and compared with the other authors' investigations. Finally, the general authors' hypothesis has been confirmed. The tested deniable encryption algorithms productivity has been increased.

Keywords: denied encryption; information protection; confidential data; divide and rule method; unauthorized access; coercion; productivity; data compression; code....

А.В. ГАЛЬЧЕНКО, С.В. ЧОПОРОВ
Запорожский национальный университет

КОДИРОВАНИЕ ДАННЯХ В АЛГОРИТМАХ ОТРИЦАЕМОГО ШИФРОВАНИЯ

Данное исследование проведено авторами для проверки гипотезы о возможности увеличения скорости работы алгоритмов отрицаемого шифрования, без внесения изменений непосредственно в исходные алгоритмы. Указанное исследование является актуальным, поскольку алгоритмы отрицаемого шифрования имеют эффективные схемы для защиты информации, ее пользователей. Однако структура указанных алгоритмов сложная и сосредоточена, что достаточно сильно влияет на скорость их работы и делает невозможным практическое применение алгоритмов отрицаемого шифрования данных для решения задач по защите информации. Основной целью исследования является обзор алгоритмов кодирования информации, которые позволяют манипулировать размером данных путем изменения их формы, но не информационной составляющей. Использование алгоритмов кодирования в теории должно существенно уменьшить размер данных, которые обрабатываются алгоритмами отрицаемого шифрования. Указанный подход должен обеспечить пропорциональный рост быстродействия алгоритмов отрицаемого шифрования и создать условия для их практического использования в дальнейшем. В этой работе выполнен обзор эффективных алгоритмов кодирования данных и их применение в процедурах обработки информации алгоритмов отрицаемого шифрования. Во время исследований были рассмотрены два алгоритма. Первый из них является базовой моделью для блочного шифрования данных с использованием механизмов отрицаемого шифрования, недостатки безопасности в его работе были обнаружены и исследованы. Другой алгоритм построен на основе имплементации эффективных алгоритмов кодирования информации в подсистему обработки данных базовой модели. Эффективность работы обоих алгоритмов была проверена на реальных файлах с публичной и секретной информацией. Исследование проводилось на стендовом аппаратном и программном обеспечении, которое имитирует рабочее место пользователя. Результаты экспериментов показывают появление прироста в скорости выполнения исходного алгоритма отрицаемого шифрования данных за счет

10.32782/KNTU2618-0340/2020.3.2-1.6

уменьшения размера входных данных. Дополнительно исследована зависимость полученных результатов от ключей шифрования разного размера. Авторы сравнили полученные результаты с исследованиями других авторов. Учитывая результаты экспериментов гипотеза авторов была подтверждена, поскольку кодирование входных данных привело к значительному сокращению их размера и соответствующего прироста скорости шифрования.

Ключевые слова: отрицаемое шифрование; защита информации; конфиденциальные данные; компрессия данных; несанкционированный доступ; принуждение; производительность; сжатие данных; шифр.

Постановка проблеми

Авторами статті створена адаптивна модель шифрування даних, яка дозволяє застосовувати будь-які алгоритми заперечуваного шифрування для обробки файлів з даними [1]. На базі вказаної моделі створено декілька варіацій багатопоточних алгоритмів шифрування даних, які демонструють досить високі показники швидкодії, в порівнянні з подібними алгоритмами [2–3]. Разом з тим автори виявили можливість додаткового скорочення розміру даних, які обробляються алгоритмами заперечуваного шифрування та впливають на продуктивність їх роботи. Для зміни форми представлення даних автори пропонують використання алгоритмів кодування інформації [4] в підсистемах обробки даних алгоритмів шифрування. На їх домку вказаний підхід дозволить скоротити розмір вхідних даних і відповідно час необхідний для їх обробки.

Аналіз останніх досліджень і публікацій

З 80-х років та до тепер фахівці різних галузей займаються питаннями розробки, впровадження та дослідження механізмів заперечуваного шифрування. За вказаний час була розроблена та досліджена значна кількість алгоритмів заперечуваного шифрування. Однак в основі концепції заперечуваного шифрування лежить використання великої кількості важких обчислень, оптимізацією яких науковців займають по теперішній час. Ключові дослідження з питань розробки та дослідження алгоритмів заперечуваного шифрування, на які спираються автори в своєму дослідженні викладені в [5–8].

Іншим перспективним напрямком досліджень є розробка ефективних алгоритмів обробки даних і їх вдосконалення, зокрема дослідження алгоритмів кодування (стиснення даних). Результати вказаних досліджень придатні для використання в будь-якій галузі діяльності людини, оскільки обробка даних набула значного поширення.. Найбільш актуальні питання та напрями досліджень щодо кодування інформації викладені в роботах [9–12].

Мета дослідження

Основною метою дослідження є пошук оптимального алгоритму кодування даних і дослідження його впливу на процедури шифрування/дешифрування даних для його подальшого використання в алгоритмах заперечуваного шифрування. Вказаний підхід повинен скоротити розмір даних та підвищити швидкість виконання процедур шифрування/дешифрування даних в алгоритмах заперечуваного шифрування.

Викладення основного матеріалу дослідження

Перед початком дослідження автори провели аналіз існуючих алгоритмів заперечуваного шифрування та інформацію стосовно продуктивності їх роботи [1]. За проведеного дослідження вторами було прийнято рішення та розроблена власна

10.32782/KNTU2618-0340/2020.3.2-1.6

ефективна модель алгоритму заперечуваного шифрування даних. Вихідний варіант запропонованого алгоритму передбачає використання окремих особливостей та конструкцій, які є типовими для існуючих симетричних алгоритмів шифрування. Особливістю вказаного рішення є те, що воно дозволяє реалізувати та використовувати будь-які механізми заперечуваного шифрування розроблені на теперішній час. Структурна схема вказаного алгоритму наведена на рис. 1:

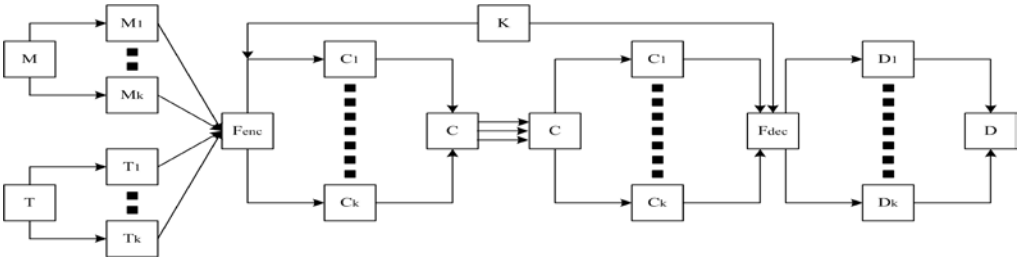


Рис. 1. Базова модель шифрування даних: $M, T, C, D, M_{1...k}, T_{1...k}, C_{1...k}, D_{1...k}$ **– позначення вихідних, шифрованих, дешифрованих даних і їх наборів,** $F_{enc}(\ldots)$ **та** $F_{dec}(\ldots)$ **– процедури шифрування та дешифрування даних,** K **– ключ шифрування.**

Метод використання механізмів заперечуваного шифрування зображений на рис. 1 демонструє досить високий рівень продуктивності в порівнянні з подібними алгоритмами [2–3]. Однак, отримані показники продуктивності недостатні для практичного використання алгоритму, в порівнянні з симетричними алгоритмами. Причиною вищевказаного є обмеження, які накладають схеми перетворення вказаних алгоритмів, та важкі обчислення, які лежать в їх основі.

Одним запропонованих авторами рішень є використання ефективних алгоритмів кодування даних. Вказане дозволить змінити форму даних і їх розмір, що є ключовим фактором для практичної реалізації алгоритмів заперечуваного шифрування.

Для використання запропонованого підходу автори розробили алгоритми імплементації ефективних алгоритмів кодування даних в підсистему обробки даних запропонованої авторами моделі (рис. 2):

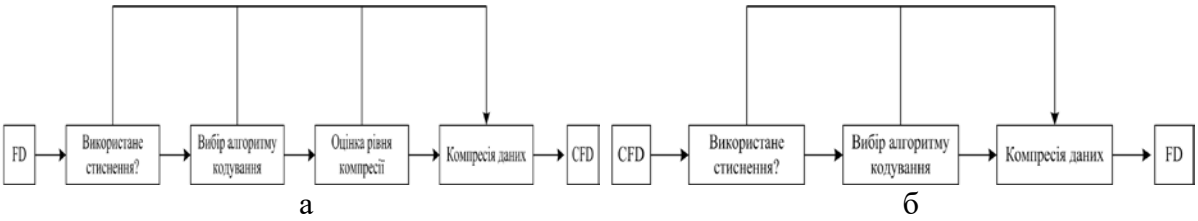


Рис. 2. Модифікація процедури обробки даних вихідного алгоритму запере чуваного шифрування: а – компресія даних; б – декомпресія даних.

Алгоритм обробки вхідних даних в процедурі шифрування (рис. 2а) включає наступний порядок дій:

1) Виконати попередню оцінку формату вхідного файлу з даними для визначення можливості використання алгоритмів кодування для їх зменшення [4].

2) Обрати ефективний алгоритм кодування даних, який відповідає типу зменшуваного файлу з даними, за класифікацією [4].

3) Знаючи розмір кодового слова після компресії даних $L_{ср}$ та значення ентропії даних H, обчислити рівень стискання файлу (1) [12]:

10.32782/KNTU2618-0340/2020.3.2-1.6

$$C_k = \frac{L_{cp} - H}{L_{cp}} \tag{1}$$

4) Виконати компресію файлу з даними за допомогою обраного алгоритму кодування інформації.

Алгоритм відновлення вхідних даних в процедурі дешифрування (рис. 2б) включає наступний порядок дій:

1) Виконати попередню перевірку файлу з даними на предмет застосування алгоритмів кодування.

2) Виконати декомпресії файлу з даними за допомогою відповідного алгоритму кодування.

Внаслідок імплементації перетворень вказаних на рис. 2 вихідна схема шифрування даних зазнала змін (рис. 3):

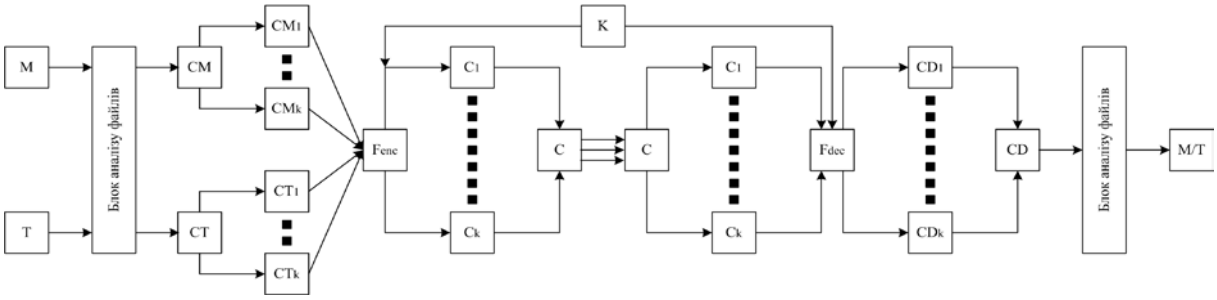


Рис. 3. Модифікована модель шифрування даних: *M, T, CM, CT, C, CD,* $M_{1..k}$, $T_{1..k}$, $CM_{1..k}$, $CT_{1..k}$, $C_{1..k}$, $CD_{1..k}$ **– позначення вихідних, стиснутих, шифрованих, дешифрованих даних і їх наборів,** $F_{enc}(\ldots)$ **та** $F_{dec}(\ldots)$ **– процедури шифрування та дешифрування даних,** K **– ключ шифрування.**

Вищевказані перетворення не змінюють базовий алгоритм, але їх використання, в теорії, повинне збільшити швидкість роботи моделі в C_k-разів.

Для проведення експериментів згідно вищевказаної схеми автори використали апаратне забезпечення – ЦП Intel(R) Core(TM) i5-8250, оперативна пам'ять DDR4 на 8 ГБ та жорсткий диск 500 ГБ; та програмне забезпечення – ОС Windows 10 та середовище програмування Python IDLE 3.7.3. Також автори внесли обмеження щодо тестових даних – розмір вхідних даних 1-20 МБ; формати тестових файлів JPG, EXE, PDF; розмір тестових ключів 1024 біт та 8192 біт. Вказані обмеження. За результатами проведених експериментів автори отримали оцінки часу роботи вихідного та модифікованого алгоритмів шифрування, які викладені в табл. 1 і 2, рис. 4.

Таблиця 1

Результати експериментів з використанням вихідної схеми

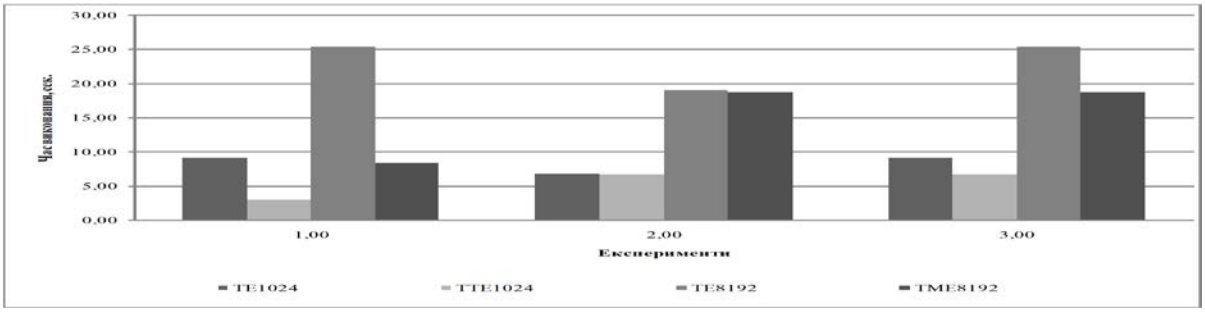
I	Формат файлів	FS, байт	TE, с		TPD, с		TSD, с	
		KS, біт	1024	8192	1024	8192	1024	8192
1	JPG	528384	9,14	25,39	1508,73	30491,33	3737,66	75538,23
	EXE	20377600						
2	JPG	528384	6,87	19,08	1133,90	22916,04	2809,07	56771,44
	PDF	15314944						
3	EXE	20377600	9,14	25,39	1508,73	30491,33	3737,66	75538,23
	PDF	15314944						

10.32782/KNTU2618-0340/2020.3.2-1.6

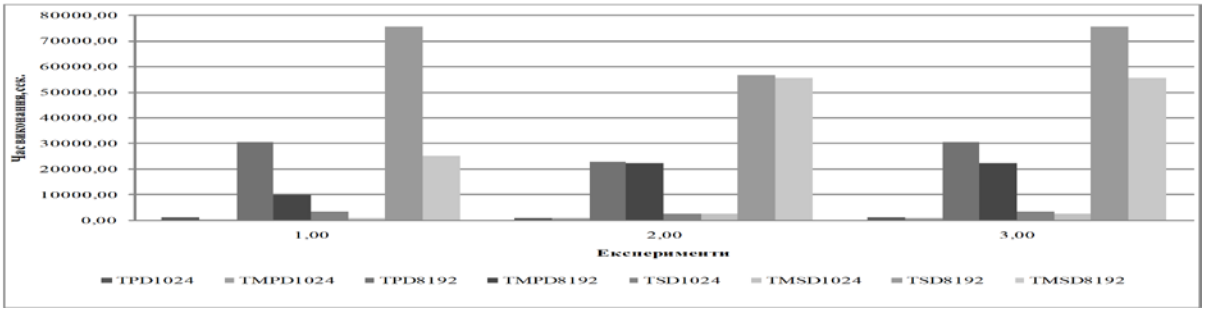
Таблиця 2

Результати експериментів з використанням модифікованої схеми

I	Формат файлів	FS, байт	TE, с		TPD, с		TSD, с	
		KS, біт	1024	8192	1024	8192	1024	8192
1	JPG	106496	3,05	8,47	503,41	10173,99	1247,14	25204,70
	EXE	6799360						
2	JPG	106496	6,74	18,72	1112,36	22480,86	2755,73	55693,34
	PDF	15024128						
3	EXE	6799360	6,74	18,72	1112,36	22480,86	2755,73	55693,34
	PDF	15024128						



а



б

Рис. 4. Оцінка часу виконання роботи вихідної і модифікованої моделей.

Результати проведених експериментів, які приведені на графіку (рис. 5) дозволяють зробити висновок, що запропонований авторами підхід призвів до незначного, але прискорення (до 3 разів прискорення алгоритмів заперечуваного шифрування). Разом з тим, вказані показники дозволили вказали авторам на необхідність повторного аналізу даних та отриманих результати, що дозволило виявити суттєву залежність коефіцієнту прискорення алгоритмів шифрування від різниці розмірів вхідних файлів. Саме тому для отримання максимальних показників прискорення в подальших дослідженнях автори рекомендують використовувати тестових дані з незначною різницею у розмірі. Також автори порівняли результати експериментів з подібними та встановили, що вказані результати хоч і не можуть порівнюватися з симетричними алгоритмами, але в порівнянні з подібними алгоритмами заперечуваного шифрування вони набагато перспективніші [2].

Висновки

В даній роботі виконано огляд основних напрямів дослідження та розробки алгоритмів заперечуваного шифрування та кодування (стиснення) даних. Авторами

10.32782/KNTU2618-0340/2020.3.2-1.6

запропонована ефективна модель шифрування даних, яка ґрунтується на використанні механізмів заперечуваного шифрування даних і їх стисненні за допомогою ефективних алгоритмів кодування. Основною метою роботи була перевірка гіпотези щодо можливості підвищення продуктивності алгоритмів заперечуваного шифрування шляхом зміни алгоритму кодування вхідних даних. Для перевірки цієї гіпотези автори провели серію експериментів, за результатами яких було отримано прискорення вихідної моделі шифрування в 1,5 – 3 рази в залежності від обраного алгоритму кодування та різниці між розмірами публічних і секретних даних. Таким чином, гіпотеза авторів була підтверджена. Результати цього дослідження можуть бути використані в дотичних дослідженнях щодо вивчення механізмів заперечуваного шифрування даних. Подальші дослідження автори планують проводити в напрямку реалізації вказаних моделей на основі багато поточних обчислень та розподілених систем, дослідження захищеності розроблених моделей.

Список використаної літератури

1. Гальченко А. В., Чопоров С. В. Заперечуване шифрування на основі застосування підходу гібридних криптографічних систем. *Радіоелектроніка, інформатика, управління*. 2019. № 1. С. 178–191.
2. Молдовян Н. А., Вайчикаускас М. А. Расширение криптосхемы Рабина: алгоритм отрицаемого шифрования по открытому ключу. *Вопросы защиты информации*. 2014. № 2. С. 12–16.
3. Молдовян Н. А., Биричевский А. Р., Мондикова Я. А. Отрицаемое шифрование на основе блочных шифров. *Информационно-управляющие системы*. 2014. № 5. С. 80–86.
4. Буза М. К. Механизм повышения надежности сжатия данных. *Штучний інтелект*. 2016. № 2. С. 96–102.
5. Goldwasser S., Micali C. Probabilistic Encryptionю. *Journal of Computer and System Sciences*. 1984. Vol. 28. P. 277–299.
6. Canetti R., Dwork C., Naor M. Ostrovsky R. Deniable Encryption. *Advances in Cryptology – CRYPTO*: 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques. (Estonia, Tallinn, May 15-19, 2011). Berlin: Springer, 1997. P. 90–104.
7. Ibrahim H. Receiver-Deniable Public-Key Encryption. *International Journal of Network Security*. 2009. Vol. 8. № 2. P. 159–165.
8. Klonowski M., Kubiak P., Kutyłowsk M. Practical Deniable Encryption. SOFSEM 2008: 34th Conference on Current Trends in Theory and Practice of Computer Science. (Slovakia, Nový Smokovec, January 19-25, 2008). Berlin: Springer, 2008. P. 599–609.
9. Лидовский В. В. Теория информации: М.: Компания Спутник+, 2004. 111 с.
10. Grasemann U., Miikkulainen R. Effective Image Compression Using Evolved Wavelets. *Genetic and Evolutionary Computation Conference, GECCO 2005*: International Conference. (USA, Washington, June 25-29, 2005). New York: Association for Computing Machinery, 2005. P. 1961–1968.
11. Zhihua G., Xiuli C., Zhang J., Zhang Y. An Effective Image Compression–Encryption Scheme Based on Compressive Sensing (CS) and Game of Life (GOL). *Neural Computing and Applications*. 2020. Vol. 32. Issue 17. P. 4961–4988.
12. Kedarnath J. B., Nur A. T. Relationship Between Entropy and Test Data Compression. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*. 2007. Vol. 26. №. 2. P. 386–395.

10.32782/KNTU2618-0340/2020.3.2-1.6

References

1. Halchenko, A. V., & Choporov, S. V. (2019). Zaperechuvane shyfruvannia na osnovi zastosuvannia pidkhodu hibrydnykh kryptohrafichnykh system. *Radioelektronika, informatyka, upravlinnia*. **1**, 178–191.
2. Moldovyan, N. A., & Vaychikauskas, M. A. (2014). Rasshirenie kriptoshemyi Rabina: algoritm otritsaemogo shifrovaniya po otkryitomu klyuchu. *Voprosyi zaschityi informatsii*. **2**, 12–16.
3. Moldovyan, N. A., Birichevskiy, A. R., & Mondikova, Ya. A. (2014). Otritsaemoe shifrovanie na osnove blochnyih shifrov. *Informatsionno-upravlyayuschie sistemyi*. **5**, 80–86.
4. Buza, M. K. (2016). Mehanizm povyisheniya nadezhnosti szhatiya dannyih. *Shtuchniy Intelekt*. **2**, 96–102.
5. Goldwasser, S., & Micali, C. (1984). Probabilistic Encryption. *Journal of Computer and System Sciences*. **28**, 277–299.
6. Canetti, R., Dwork, C., Naor, M. & Ostrovsky, R. (1997). Deniable Encryption. *Advances in Cryptology – CRYPTO*: *30th Annual International Conference on the Theory and Applications of Cryptographic Techniques*. (Estonia, Tallinn, May 15-19, 2011). Berlin: Springer, pp. 90–104.
7. Ibrahim, H. (2009). Receiver-Deniable Public-Key Encryption. *International Journal of Network Security*. **8**, 2, 159–165.
8. Klonowski M., Kubiak P., Kutyłowsk M. (2008). Practical Deniable Encryption. SOFSEM 2008: 34th Conference on Current Trends in Theory and Practice of Computer Science. (Slovakia, Nový Smokovec, January 19-25, 2008). Berlin: Springer, pp. 599–609.
9. Lidovskiy, V. V. (2004). Teoriya informatsii: Uchebnoe posobie. M.: Kompaniya Sputnik.
10. Grasemann, U., & Miikkulainen, R. (2005). Effective Image Compression Using Evolved Wavelets. *Genetic and Evolutionary Computation Conference, GECCO 2005*: International Conference. (USA, Washington, June 25-29, 2005). New York: Association for Computing Machinery, pp. 1961–1968.
11. Zhihua, G., Xiuli, C., Zhang, J., & Zhang, Y. (2020). An Effective Image Compression–Encryption Scheme Based on Compressive Sensing (CS) and Game of Life (GOL). *Neural Computing and Applications*. **32**, 17, 4961–4988.
12. Kedarnath J. B., & Nur A. T. Relationship Between Entropy and Test Data Compression. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*. **26**, 2, 386–395.

Гальченко Андрій Віталійович – аспірант кафедри програмної інженерії Запорізького національного університету, email: andream1993@ukr.net, ORCID: 0000-0002-2258-9755.

Чопоров Сергій Вікторович – к.т.н., доцент, старший викладач кафедри програмної інженерії Запорізького національного університету, e-mail: s.choporoff@znu.edu.ua , ORCID: 0000-0001-5932-952X.

10.32782/KNTU2618-0340/2020.3.2-1.6