КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3(15), 2022
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2022.15.8592
УДК 004.056

Смірнова Тетяна Віталіївна
кандидат технічних наук, доцент кафедри кібербезпеки та програмного забезпечення
Центрально український національний технічний університет, Кропивницький, Україна
ORCID ID:0000-0001-6896-0612
sm.tetyana@gmail.com

Якименко Наталія Миколаївна
кандидат фізико-математичних наук, доцент кафедри кібербезпеки та програмного забезпечення
Центральноукраїнський національний технічний університет, Кропивницький, Україна
ORCID ID: 0000-0002-4498-0093
yakimenko_n_m@ukr.net

Улічев Олександр Сергійович
кандидат технічних наук, старший викладач кафедри кібербезпеки та програмного забезпечення
Центральноукраїнський національний технічний університет, Кропивницький, Україна
ORCID ID: 0000-0003-3736-9613
askin79@gmail.com

Конопліцька-Слободенюк Оксана Костянтинівна
викладач кафедри кібербезпеки та програмного забезпечення
Центральноукраїнський національний технічний університет, Кропивницький, Україна
ORCID ID: 0000-0001-9981-5194
ksuha80@gmail.com

Смірнов Сергій Анатолійович
кандидат технічних наук, доцент кафедри кібербезпеки та програмного забезпечення
Центральноукраїнський національний технічний університет, Кропивницький, Україна
ORCID ID: 0000-0002-7649-7442
smirnov.ser.81@gmail.com

ДОСЛІДЖЕННЯ ЛІНІЙНИХ ПЕРЕТВОРЕНЬ ЗАПРОПОНОВАНОЇ ФУНКЦІЇ ГЕШУВАННЯ УДОСКОНАЛЕНОГО МОДУЛЯ КРИПТОГРАФІЧНОГО ЗАХИСТУ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ

Анотація. У даній роботі проведено дослідження лінійних перетворень функції гешування, яка є складовою розробленого удосконаленого модулю криптографічного захисту інформації, який за рахунок фіксування інформації про ідентифікатор користувача, ідентифікатор сесії, час відправлення, довжини повідомлення та його порядковий номер, а також використання нової процедури формування сеансового ключа для шифрування, дозволяє забезпечити конфіденційність і цілісність даних в інформаційно-комунікаційних системах управління технологічними процесами. Об'єктом дослідження є процес забезпечення конфіденційності даних в інформаційно-комунікаційних системах управління технологічними процесами на базі хмарних технологій. Предметом є дослідження лінійних перетворень запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах. Метою даної роботи є дослідження лінійних перетворень запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах управління технологічними процесами на базі хмарних технологій. Для ефективного використання цього модуля важливим є вибір криптостійких методів шифрування та гешування, а також синхронізація секретного ключа. У якості функцій криптостійких методів шифрування та гешування можуть бути використані криптоалгоритми, стійкі до лінійного, диференціального, алгебраїчного, квантового та інших відомих видів криптоаналізу. Проведене експериментальне дослідження лінійних перетворень запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах підтвердило криптостійкість удосконаленого алгоритму до лінійного криптоаналізу.

Ключові слова: лінійні перетворення, функція гешування.

ВСТУП

Початок 2022 року в України ознаменувався рядом кібератак на хмарні ресурси державних установ. Так під час масованої кібератаки, яка почалася у ніч з 13-го на 14 січня, постраждали 22 сайти органів державної влади. Шести сайтам було завдано значної шкоди, 70 – відключено за вказівкою Держспецзв'язку та Служби безпеки України [1]. Починаючи з другої половини дня 15 лютого 2022 року спостерігалась потужна DDoS-атака на низку інформаційних ресурсів України. Зокрема, було зафіксовано перебої в роботі веб-сервісів Приватбанку та Ощадбанку. Також атаки зазнали сайти Міністерства оборони та Збройних Сил України [2]. Таким чином очевидно, що на сучасному етапі розвитку хмарних технологій, існує завдання захисту даних, які зберігаються у відповідних інформаційно-комунікаційних системах. Останні події, пов'язані з атаками на різні хмарні сервіси потребують розроблення нових або удосконалення існуючих механізмів захисту інформації. Одними з таких механізмів є програмні модулі криптографічного захисту даних, у яких необхідно реалізовувати вибір стійких методів шифрування та гешування, а також синхронізацію секретного ключа. У якості зазначених процедур можуть використовуватись відомі криптографічні методи і засоби, стійкі до лінійного, диференціального, алгебраїчного, квантового та інших відомих видів криптоаналізу.

АНАЛІЗ ПУБЛІКАЦІЙ ТА ПОСТАНОВКА ЗАВДАННЯ ДОСЛІДЖЕННЯ

Сьогодні серед множини методів захисту інформації особливе місце займають криптографічні методи [3]. У теперішній час в хмарних сервісах використовуються наступні відомі програмні модулі криптографічного захисту даних: MTProto 1.0 [4] – модуль, який використовується для шифрування повідомлень при передаванні клієнтами Telegram; Signal Protocol [5] – використовується для шифрування миттєвих повідомлень Facebook Messenger; TLS Skype [6] – для миттєвих повідомлень використовується TLS (безпека на рівні транспорту) для шифрування повідомлень між клієнтом Skype та службою чату, коли вони надсилаються безпосередньо між двома клієнтами Skype. Проведений порівняльний аналіз розглянутих модулів захисту інформації у сучасних інформаційно-комунікаційних системах та мережах (ІКСМ). за такими критеріями, як використовувані криптоалгоритми, швидкість роботи (ШР), зручність для користувачів (ЗК) і кросплатформеність (КП), показав, що розглянуті програмні модулі мають низку недоліків і можуть бути удосконалені за рахунок використання сучасних процедур безпеки [16]. Зважаючи на зазначене, в роботі [16] був розроблений удосконалений модуль криптографічного захисту інформації для забезпечення конфіденційності та цілісності даних у сучасних ІКСМ. Для використання цього модуля на практиці потрібно визначитись з функціями гешування F_{hash} та шифрування F_{enc}. Удосконалений модуль криптографічного захисту інформації, за рахунок фіксування інформації про ідентифікатор користувача, ідентифікатор сесії, час відправлення, довжину повідомлення та його порядковий номер, а також використання нової процедури формування сеансового ключа для шифрування, дозволяє забезпечити конфіденційність і цілісність даних в ІКСМ [16]. Для ефективного використання цього модуля важливим є вибір криптостійких методів шифрування F_{enc} та гешування F_{hash}, а також синхронізація секретного ключа $authKey$. У якості функцій F_{enc} та F_{hash} можуть бути використані зокрема й алгоритми, запропоновані авторами у своїх попередніх

роботах [8, 10-12, 16], або інші відомі криптоалгоритми [7, 9, 13-15], стійкі до лінійного, диференціального, алгебраїчного, квантового та інших відомих видів криптоаналізу. У подальшому планується зосередити увагу на дослідженнях удосконаленого модуля криптографічного захисту інформації з використанням різних методів шифрування і гешування, зокрема тих, що були запропоновані авторами у своїх попередніх дослідженнях. Областю застосування запропонованих підходів є хмарні системи які описані у [19-20].

Методи дослідження. Основні теоретичні положення роботи отримані з використанням методів теорії захисту інформації.

Об'єктом дослідження є процес забезпечення конфіденційності даних в інформаційно-комунікаційних системах управління технологічними процесами на базі хмарних технологій.

Предметом є дослідження лінійних перетворень запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах.

Метою даної роботи є дослідження лінійних перетворень запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах управління технологічними процесами на базі хмарних технологій.

ОСНОВНА ЧАСТИНА ДОСЛІДЖЕННЯ

Теоретичне обґрунтування удосконалення модуля захисту

З огляду на результати проведеного аналізу, прототипом було обрано розглянутий модуль MTProto Mobile Protocol v.1.0 [4], порівняно з яким було змінено наступне [16]:

1. Змінені вхідні та вихідні дані. На вході приймаються і обробляються наступні дані: повідомлення M, інформацію про ідентифікатор користувача та ідентифікатор сесії S, інформацію про час відправлення і довжину повідомлення ID та порядковий номер повідомлення PD. На виході тільки отримуємо $mHash$ – геш значення DB ($DB = (S, ID, M)$) та $EncP$ – зашифроване повідомлення P [16].

2. Замість використання геш функції SHA-1 введено використання певної криптостійкої геш функції F_{hash}. Слід зауважити, що у якості F_{hash} може бути використана функція гешування, що побудована на основі одного із методів [7-9, 16].

3. Замість використання блокового шифру AES введено використання функції F_{enc}. Слід зауважити, що у якості F_{enc} може бути використаний певний криптостійкий алгоритм шифрування, побудований на основі блокових, потокових шифрів чи геш функцій тощо [10-12, 16].

4. У якості $authKey$, введено використання заздалегідь узгодженого секретного ключа користувачів, наприклад за допомогою протоколів асиметричної криптографії [16].

Для використання цього модуля на практиці потрібно визначитись з функціями гешування F_{hash} та шифрування F_{enc}.

Дослідження лінійних перетворень запропонованої функції гешування для забезпечення удосконаленого модуля криптографічного захисту

Багато видів криптоаналітичних атак засновані на лінійності більшості перетворень, що використовуються у шифрах. Під лінійним перетворенням T відносно деякої операції $\oplus$. розуміється перетворення, для якого справедливо

$$T(X)\oplus T(X') = T(X\oplus X'),$$

де $T(X)$ – результат виконання перетворення T для вхідного блоку X.

Лінійні перетворення в БСШ вирішують завдання розсіювання, тобто поширюють вплив кожного вхідного біта на як можна більшу кількість вихідних бітів. Основний показник, що характеризує якість розсіювання лінійного перетворення, це число галузей активізації (branch number) [7]. Число галузей активізації B для лінійного перетворення T визначається як:

$$B = \min_{X=0}\Big(W(X) + W\big(T(X)\big)\Big)$$

де X – значення на вході лінійного перетворення, $T(X)$ – результат застосування лінійного перетворення, $W(X)$ – функція, що визначає число ненульових байтів (бітів) в X.

Чим більше число галузей активізації перетворення розсіювання, тим швидше відбувається поширення впливу кожного вхідного біта на вихідні біти при виконанні перетворень шифру та тим складніше буде встановити кореляційну залежність між бітами на вході та виході шифру.

Серед лінійних перетворень сьогодні широке застосування одержали перетворення на основі МДР-кодів (коди з максимально-допустимою відстанню). Подібні перетворення використовуються в шифрах Rijndael, Hierocrypt, Khazad, Anubis, Square. Головна перевага лінійних перетворень цього класу полягає в тому, що гарантується максимально досяжне число галузей активізації. Тобто якщо МДР-перетворення покриває M байтів, то $B = M + 1$ байт.

Можна зробити висновок, що число галузей активізації для лінійних перетворень шифру NRC21 дорівнює 9.

Важливий показник для оцінки стійкості шифру до диференціального та лінійного криптоаналізу – це мінімальна кількість активних підстановок. Значення цього показника багато в чому визначається числом галузей активізації для перетворень, що використовуються, але при розгляді багатоциклових перетворень необхідний більш ретельний аналіз цього показника.

Відповідно до принципів проведення диференціального та лінійного криптоаналізу шифру «Калина» [12], справедливе твердження 1.

Твердження 1. Окремий цикл шифру NRC21 завжди містить хоча б одну активну підстановку.

Відповідно до загальної кількості активних підстановок справедливе твердження 2.

Твердження 2. Будь-який цикл шифру NRC21 з 128-бітним блоком не може містити більше 16 активних підстановок.

Ґрунтуючись на тому, що число галузей активізації лінійних перетворень шифру NRC21 дорівнює 9, то справедливе твердження 3.

Твердження 3. Мінімальна кількість активних підстановок у будь-яких двох сусідніх циклах шифру NRC21 буде не менше, ніж 9.

У результаті детального розгляду, для перетворень, які використовуються в шифрі NRC21, доведено твердження 1.

Твердження 4. Для шифру з n_c колонками та n_r рядками (n_r кратне n_c) і з байтовою перестановкою, що розподіляє байти кожної колонки нарівно серед всіх

ISSN 2663 - 4023

колонок, мінімальне число активних підстановок (S-блоків) в 4-цикловій диференціальній або лінійній характеристиці буде не менш, ніж $(n_c + 1) - (n_r + 1)$.

Ґрунтуючись на твердженнях 1-4 можна визначити мінімальну кількість активних підстановок для різних варіантів шифру NRC21 (див. табл. 1).

Таблиця 1

Розрахована мінімальна кількість активних підстановок для зазначеної кількості раундів

Розмір блоку, біти	Число циклів									
	1	2	3	**4**	5	6	7	**8**	9	10
128	1	9	11	**27**	28	36	38	**54**	55	63
Розмір блоку, біти	Число циклів									
	11	**12**	13	14	15	**16**	17	18	19	**20**
128	65	**81**	82	90	92	**108**	109	117	119	**135**

При заповненні табл. 1, спочатку були заповнені осередки, що відповідають циклам з номерами $4i$ (номера циклів кратні 4). Значення цих осередків обчислені відповідно до твердження 4 (значення в цих осередках виділені жирним шрифтом). Значення осередків для кількості циклів $4i + 1$ обчислені відповідно до твердження 1: значення в цих осередках дорівнюють значенням в осередках $4i$ плюс 1. Значення осередків для кількості циклів $4i + 2$ обчислені відповідно до твердження 3: значення в цих осередках дорівнюють значенням в осередках $4i$ плюс 9. Значення осередків для кількості циклів $4i + 3$ обчислені відповідно до твердження 2: значення в цих осередках дорівнюють значенням в осередках $4(i + 1)$ мінус 16 для 128-бітного блоку.

Результати, що наведені в табл. 1 надалі будуть використані при оцінці стійкості шифру NRC21 до диференціального та лінійного криптоаналізу.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Удосконалено модуль криптографічного захисту інформації, який за рахунок фіксування інформації про ідентифікатор користувача, ідентифікатор сесії, час відправлення, довжину повідомлення та його порядковий номер, а також використання нової процедури формування сеансового ключа для шифрування, дозволяє забезпечити конфіденційність і цілісність даних в ІКСМ управління технологічними процесами. Для ефективного використання цього модуля важливим є вибір криптостійких методів шифрування F_{enc} та гешування F_{hash}, а також синхронізація секретного ключа $authKey$. У якості функцій F_{enc} та F_{hash} можуть бути використані криптоалгоритми, стійкі до лінійного, диференціального, алгебраїчного, квантового та інших відомих видів криптоаналізу. Проведено дослідження лінійних перетворень запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах. Проведене експериментальне дослідження підтвердило криптостійкість удосконаленого алгоритму до лінійного криптоаналізу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 *Кабінет Міністрів України - Від кібератаки 14 січня постраждали 22 державних органи, - Держспецзв'язку*. (б. д.). Головна | Кабінет Міністрів України. https://www.kmu.gov.ua/news/vid-kiberataki-14-sichnya-postrazhdali-22-derzhavnih-organi-derzhspeczvyazku

2 *Кабінет Міністрів України - Щодо кібератаки на сайти військових структур та державних банків*. (б. д.). Головна | Кабінет Міністрів України. https://www.kmu.gov.ua/news/shchodo-kiberataki-na-sajti-vijskovih-struktur-ta-derzhavnih-bankiv

3 Oppliger, R. (2021). *Cryptography 101: From Theory to Practice*. Artech.

4 Job J, Naresh V, Chandrasekaran, K. (2015). A modified secure version of the Telegram protocol (MTProto). У *2015 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT)*. IEEE. https://doi.org/10.1109/conecct.2015.7383884

5 Dion van D. (2019). Analysing the Signal Protocol. A manual and automated analysis of the Signal Protocol.

6 Skype. (2011). *TLS and SRTP for Skype Connect Technical Datasheet*.

7 Wu, Q. (2015). A Chaos-Based Hash Function. У *International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery* (с. 1–4).

8 Gnatyuk, S., Kinzeryavyy, V., Kyrychenko, K., Yubuzova, K., Aleksander, M., & Odarchenko, R. (2019a). Secure Hash Function Constructing for Future Communication Systems and Networks. У *Advances in Artificial Systems for Medicine and Education II* (с. 561–569). Springer International Publishing. https://doi.org/10.1007/978-3-030-12082-5_51.

9 Rajeshwaran, K., & Anil Kumar, K. (2019a). Cellular Automata Based Hashing Algorithm (CABHA) for Strong Cryptographic Hash Function. У *2019 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT)*. IEEE. https://doi.org/10.1109/icecct.2019.8869146

10 Iavich, M., Iashvili, G., Gnatyuk, S., Tolbatov, A., Mirtskhulava, L. (2021). Efficient and Secure Digital Signature Scheme for Post Quantum Epoch. *Communications in Computer and Information Science*, (1486), 185-193.

11 Gnatyuk, S., Iavich, M., Kinzeryavyy, V., Okhrimenko, T., Burmak, Y., Goncharenko, I. (2020). Improved secure stream cipher for cloud computing. *CEUR Workshop Proceedings*, (2732), 183-197.

12 Gnatyuk, S., Akhmetov, B., Kozlovskyi, V., Kinzeryavyy, V., Aleksander, M., & Prysiazhnyi, D. (2020). New Secure Block Cipher for Critical Applications: Design, Implementation, Speed and Security Analysis. У *Advances in Intelligent Systems and Computing* (с. 93–104). Springer International Publishing. https://doi.org/10.1007/978-3-030-39162-1_9.

13 Kuznetsov, A., Horkovenko, I., Maliy, O., Goncharov, N., Kuznetsova, T., & Kovalenko, N. (2020b). Non-Binary Cryptographic Functions for Symmetric Ciphers. У *2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T)*. IEEE. https://doi.org/10.1109/picst51311.2020.9467982.

14 Jintcharadze, E., Iavich, M. (2020). Hybrid Implementation of Twofish, AES, ElGamal and RSA Cryptosystems. У *2020 IEEE East-West Design & Test Symposium (EWDTS)*. IEEE. https://doi.org/10.1109/ewdts50664.2020.9224901.

15 Lee, T. R., Teh, J. S., Jamil, N., Yan, J. L. S., Chen, J. (2021). Lightweight Block Cipher Security Evaluation Based on Machine Learning Classifiers and Active S-Boxes. In *IEEE Access*, 9, 134052-134064. doi: 10.1109/ACCESS.2021.3116468.

16 Смірнова, Т.В., Гнатюк, С.О., Бердибаєв, Р.Ш., Бурмак, Ю.А., Оспанова, Д.М. (2021). Удосконалений модуль криптографічного захисту інформації в сучасних інформаційно-комунікаційних системах та мережах. *Кібербезпека: освіта, наука, техніка*, *2*(14), 176-185.

17 Смірнова, Т.В., Поліщук, Л.І., Смірнов, О.А., Буравченко, К.О., Макевнін, А.О. (2020). Дослідження хмарних технологій як сервісів. *Кібербезпека: освіта, наука, техніка*, *3*(7), 43-62.

18 Смірнова, Т.В., Солових, Є.К., Смірнов, О.А., Дрєєв, О.М. (2019). Побудова хмарних інформаційних технологій оптимізації технологічного процесу відновлення та зміцнення поверхонь деталей. *Центральноукраїнський науковий вісник. Технічні науки*, *1*(32), 184-194.

19 Смірнова, Т.В., Смірнов, С.А., Минайленко, Р.М., Доренський, О.П., Сисоєнко, С.В. (2020). Хмарна автоматизована система інтелектуальної підтримки прийняття рішень для технологічних процесів. *Вісник Черкаського державного технологічного університету. Технічні науки*, *4*, 84-92.

20 Смірнова, Т.В., Буравченко, К.О., Кравченко, С.С., Горбов, В.О., Смірнов, О.А. (2021). Хмарна система підтримки прийняття рішень технологічного процесу відновлення поверхонь конструкцій і деталей машин. *Сучасні інформаційні системи*, *5*(4), 79-95.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (15), 2022
ISSN 2663 - 4023

Tetiana Smirnova
Candidate of Science (Engineering), Associate Professor of Cybersecurity & Software Academic Department
Central Ukrainian National Technical University, Kropyvnytskyi, Ukraine
ORCID ID:0000-0001-6896-0612
sm.tetyana.gmail.com

Nataliia Yakymenko
Candidate of Physical and Mathematical Sciences, Associate Professor of Cybersecurity & Software Academic Department
Central Ukrainian National Technical University, Kropyvnytskyi, Ukraine
ORCID ID: 0000-0002-4498-0093
yakimenko_n_m@ukr.net

Oleksandr Ulichev
Candidate of Science (Engineering), Senior Lecturer of Cybersecurity & Software Academic Department
Central Ukrainian National Technical University, Kropyvnytskyi, Ukraine
ORCID ID: 0000-0003-3736-9613
askin79@gmail.com

Oksana Konoplitska-Slobodeniuk
lecturer of Cybersecurity & Software Academic Department
Central Ukrainian National Technical University, Kropyvnytskyi, Ukraine
ORCID ID: 0000-0001-9981-5194
ksuha80@gmail.com

Serhii Smirnov
Candidate of Science (Engineering), Associate Professor of Cybersecurity & Software Academic Department
Central Ukrainian National Technical University, Kropyvnytskyi, Ukraine
ORCID ID: 0000-0002-7649-7442
smirnov.ser.81@gmail.com

INVESTIGATION OF LINEAR TRANSFORMATIONS OF THE PROPOSED HUSHING FUNCTION OF THE ADVANCED MODULE OF CRYPTOGRAPHIC PROTECTION IN INFORMATION AND CIRCUMSTANCES

Abstract. This paper investigates the linear transformations of the hash function, which is part of the developed advanced module of cryptographic protection of information, which by capturing information about the user ID, session ID, sending time, message length and sequence number, as well as using a new session key generation procedure for encryption, allows you to ensure the confidentiality and integrity of data in information and communication systems process control. The object of research is the process of ensuring the confidentiality of data in information and communication systems management systems based on cloud technologies. The subject is the study of linear transformations of the proposed hashing function of the advanced module of cryptographic protection in information and communication systems. The purpose of this work is to study the linear transformations of the proposed hashing function of the advanced module of cryptographic protection in information and communication systems for process control based on cloud technologies. To use this module effectively, it is important to choose crypto-resistant encryption and hashing methods, as well as secret key synchronization. Cryptoalgorithms resistant to linear, differential, algebraic, quantum and other known types of cryptanalysis can be used as functions of cryptographic methods of encryption and hashing. The conducted experimental study of linear transformations of the proposed hashing function of the advanced module of cryptographic protection in information and communication systems confirmed the cryptoresistance of the advanced algorithm to linear cryptanalysis.

Keywords: linear transformations, hashing function.

REFERENCES

1 Kabinet Ministriv Ukrainy - Vid kiberataky 14 sichnia postrazhdaly 22 derzhavnykh orhany, - Derzhspetszviazku. Holovna | Kabinet Ministriv Ukrainy. https://www.kmu.gov.ua/news/vid-kiberataki-14-sichnya-postrazhdali-22-derzhavnih-organi-derzhspeczvyazku

2 Kabinet Ministriv Ukrainy - Shchodo kiberataky na saity viiskovykh struktur ta derzhavnykh bankiv. Holovna | Kabinet Ministriv Ukrainy. https://www.kmu.gov.ua/news/shchodo-kiberataki-na-sajti-vijskovih-struktur-ta-derzhavnih-bankiv

3 Oppliger, R. (2021). *Cryptography 101: From Theory to Practice*. Artech.

4 Job J, Naresh V, Chandrasekaran, K. (2015). A modified secure version of the Telegram protocol (MTProto). У *2015 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT)*. IEEE. https://doi.org/10.1109/conecct.2015.7383884

5 Dion van D. (2019). Analysing the Signal Protocol. A manual and automated analysis of the Signal Protocol.

6 Skype. (2011). *TLS and SRTP for Skype Connect Technical Datasheet*.

7 Wu, Q. (2015). A Chaos-Based Hash Function. У *International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery* (с. 1–4).

8 Gnatyuk, S., Kinzeryavyy, V., Kyrychenko, K., Yubuzova, K., Aleksander, M., & Odarchenko, R. (2019a). Secure Hash Function Constructing for Future Communication Systems and Networks. In *Advances in Artificial Systems for Medicine and Education II* (с. 561–569). Springer International Publishing. https://doi.org/10.1007/978-3-030-12082-5_51.

9 Rajeshwaran, K., & Anil Kumar, K. (2019a). Cellular Automata Based Hashing Algorithm (CABHA) for Strong Cryptographic Hash Function. У *2019 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT)*. IEEE. https://doi.org/10.1109/icecct.2019.8869146

10 Iavich, M., Iashvili, G., Gnatyuk, S., Tolbatov, A., Mirtskhulava, L. (2021). Efficient and Secure Digital Signature Scheme for Post Quantum Epoch. *Communications in Computer and Information Science*, (1486), 185-193.

11 Gnatyuk, S., Iavich, M., Kinzeryavyy, V., Okhrimenko, T., Burmak, Y., Goncharenko, I. (2020). Improved secure stream cipher for cloud computing. *CEUR Workshop Proceedings*, (2732), 183-197.

12 Gnatyuk, S., Akhmetov, B., Kozlovskyi, V., Kinzeryavyy, V., Aleksander, M., & Prysiazhnyi, D. (2020). New Secure Block Cipher for Critical Applications: Design, Implementation, Speed and Security Analysis. У *Advances in Intelligent Systems and Computing* (с. 93–104). Springer International Publishing. https://doi.org/10.1007/978-3-030-39162-1_9.

13 Kuznetsov, A., Horkovenko, I., Maliy, O., Goncharov, N., Kuznetsova, T., & Kovalenko, N. (2020b). Non-Binary Cryptographic Functions for Symmetric Ciphers. У *2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T)*. IEEE. https://doi.org/10.1109/picst51311.2020.9467982.

14 Jintcharadze, E., Iavich, M. (2020). Hybrid Implementation of Twofish, AES, ElGamal and RSA Cryptosystems. У *2020 IEEE East-West Design & Test Symposium (EWDTS)*. IEEE. https://doi.org/10.1109/ewdts50664.2020.9224901.

15 Lee, T. R., Teh, J. S., Jamil, N., Yan, J. L. S., Chen, J. (2021). Lightweight Block Cipher Security Evaluation Based on Machine Learning Classifiers and Active S-Boxes. In *IEEE Access*, 9, 134052-134064. doi: 10.1109/ACCESS.2021.3116468.

16 Smirnova, T.V., Hnatiuk, S.O., Berdybaiev, R.Sh., Burmak, Yu.A., Ospanova, D.M. (2021). Udoskonalenyi modul kryptohrafichnoho zakhystu informatsii v suchasnykh informatsiino-komunikatsiinykh systemakh ta merezhakh. Kiberbezpeka: osvita, nauka, tekhnika, 2(14), 176-185.

17 Smirnova, T.V., Polishchuk, L.I., Smirnov, O.A., Buravchenko, K.O., Makevnin, A.O. (2020). Doslidzhennia khmarnykh tekhnolohii yak servisiv. Kiberbezpeka: osvita, nauka, tekhnika, 3(7), 43-62.

18 Smirnova, T.V., Solovykh, Ye.K., Smirnov, O.A., Drieiev, O.M. (2019). Pobudova khmarnykh informatsiinykh tekhnolohii optymizatsii tekhnolohichnoho protsesu vidnovlennia ta zmitsnennia poverkhon detalei. Tsentralnoukrainskyi naukovyi visnyk. Tekhnichni nauky, 1(32), 184-194.

19 Smirnova, T.V., Smirnov, S.A., Mynailenko, R.M., Dorenskyi, O.P., Sysoienko, S.V. (2020). Khmarna avtomatyzovana systema intelektualnoi pidtrymky pryiniattia rishen dlia tekhnolohichnykh protsesiv. Visnyk Cherkaskoho derzhavnoho tekhnolohichnoho universytetu. Tekhnichni nauky, 4, 84-92.

20 Smirnova, T.V., Buravchenko, K.O., Kravchenko, S.S., Horbov, V.O., Smirnov, O.A. (2021). Khmarna systema pidtrymky pryiniattia rishen tekhnolohichnoho protsesu vidnovlennia poverkhon konstruktsii i detalei mashyn. Suchasni informatsiini systemy, 5(4), 79-95.