КОМП'ЮТЕРНІ НАУКИ, ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ, СИСТЕМНИЙ АНАЛІЗ ТА КІБЕРБЕЗПЕКА

DOI 10.31891/2307-5732-2021-293-1-7-11
УДК 004.421.5:004.942

О.С. АНДРОЩУК, Ю.П. КЛЬОЦ, В.С. ОРЛЕНКО, В.М. ЧЕШУН
Хмельницький національний університет
Т.М. КОРОТУН
Заклад вищої освіти "Міжнародний науково-технічний університет імені академіка Юрія Бугая"

ФУНКЦІОНАЛЬНА РЕАЛІЗАЦІЯ ГЕНЕРАТОРА КРИПТОКЛЮЧІВ З ДЖЕРЕЛАМИ ЕНТРОПІЇ ДЛЯ МОБІЛЬНОГО БАНКІНГУ

В роботі представлено опис базових принципів використання датчиків пристроїв мобільного зв'язку в якості джерел первинної ентропії генераторів криптоключів системи клієнт-банк при наданні послуг мобільного банкінгу, визначено процедуру накопичення і обробки пулу ентропії, уточнено основні функції процедури та приведено деталізовану функціональну модель процесу генерації криптоключів. Отримані результати дають можливість виконати деталізацію алгоритму роботи системи клієнт-банк із застосуванням генераторів криптоключів підвищеної ентропії в мобільному банкінгу та інших сервісах.

Ключові слова: алгоритм, мобільний банкінг, криптографічний ключ, генератор псевдовипадкових чисел, ентропія.

O.S. ANDROSHCHUK, Y.P. KLOTS, V.S. ORLENKO, V.M. CHESHUN
Khmelnytskyi National University
T.M. KOROTUN
Academician Yuriy Bugay International Scientific and Technical University

FUNCTIONAL REALIZATION OF CRYPTOGRAPHIC KEYS GENERATOR WITH ENTROPY SOURCES FOR MOBILE BANKING

One of the important components of the security of the client-bank system is the protection mechanisms based on the use of cryptographic keys. The stability of cryptographic keys is a guarantee of system reliability and, in turn, is based on the mechanisms of generating pseudo-random numbers using primary entropy sources, for the effective use of which it is necessary to define and describe the functions of the algorithm for data processing.

The paper describes the basic principles of using sensors of mobile devices as primary entropy sources for cryptographic keys generators of the client-bank system in the provision of mobile banking services, defines the procedure for accumulation and processing of entropy pool from sensors, described the main functions of the procedure and detailed functional model the process of generating cryptographic keys. The obtained results make it possible to perform a detailed algorithm of the client-bank system with the use of high-entropy cryptographic keys generators in mobile banking and other services.

The obtained results are focused on the implementation of algorithms and means of generating pseudo-random numbers of high entropy and can be used to reduce the risks of unauthorized access to customer information in the client-bank system through the disclosure of cryptokeys in mobile banking services. Mobile phone sensors or other devices and phenomena that are characterized by the a bility to form a pool of values with a high level of entropy can be used as sources of entropy.

Keywords: algorithm, mobile banking, cryptographic key, pseudo-random number generator, entropy.

Вступ

Історія банківської діяльності протягом сторічь нерозривно пов'язується з фінансовими злочинами. Відповідно, з моменту започаткування банківської діяльності виникла потреба в оцінці наявних загроз та ризиків з подальшим визначенням методів та засобів захисту.

В епоху суцільної комп'ютеризації, інформатизації, глобалізації і науково-технічного прогресу банківська діяльність отримала потужний потенціал вдосконалення: постійно нарощується перелік послуг, розширюється спектр банківських сервісів, впроваджуються новітні системи обслуговування, вдосконалюються технології захисту. Сучасна банківська система – надскладний механізм, в якому задіяно величезну кількість співробітників та використовуються різноманітні технології, але запровадження нових сервісів та технологій нерозривно пов'язане з появою нових загроз та ризиків [1].

Намагання банків утримувати лідерські позиції в умовах жорсткої конкуренції зумовлює їх зацікавленість у якнайшвидшому впровадженні нових технологій і систем, що призводить до жорсткого обмеження на строки випробування подібних систем і до ризиків виникнення вад в процедурах їх захисту, якими успішно користуються зловмисники. За надійність електронних систем захисту банківської інформації сьогодні відповідають колективи фахівців з інформаційної та кібербезпеки, діяльність яких є досить вузькоспеціалізованою через велику складність організації систем безпеки, різноманіття застосовуваних в них методів і засобів, потребу врахування багатьох аспектів вирішуваних завдань та застосування останніх досягнень науки і практики в сфері захисту інформації.

Однією із спеціалізованих задач кібербезпеки банківської діяльності, якій постійно приділяється велика увага, є генерація криптоключів високої криптостійкості для систем клієнт-банк як одного з головних засобів захисту клієнтських даних і активів.

Аналіз останніх досліджень і публікацій

Особливістю сучасної банківської діяльності є різноманіття сервісів банківських послуг, які орієнтовані на використання різноманітних технологій і засобів організації взаємодії клієнт-банк [2]. Відповідно, в кожній задачі кіберзахисту банківської діяльності повинні враховуватись специфіки зазначених сервісів і технологій їх реалізації. Неможливо уявити якісного генератора криптоключів, розробленого без урахування специфічних особливостей і можливостей засобів генерації та експлуатації цих ключів.

До типових сервісів сучасних банківських послуг відносять комп'ютерний банкінг (PC banking), телефонний банкінг (Phone banking), SMS-банкінг (SMS banking), WAP-банкінг (WAP banking), мобільний банкінг (Mobile banking), Internet-банкінг (Internet banking, WEB banking, Online banking) тощо [2–4]. Особливе місце серед банківських сервісів в сучасних умовах займає мобільний банкінг, який набуває все більшої популярності і поширення. З наведеного переліку видно, що мобільний банкінг існує не лише як самостійний сервіс (Mobile banking) – з використанням мобільного зв'язку реалізується цілий ряд інших сервісів (SMS banking, WAP banking тощо). З іншої сторони, за наданою в [5] класифікацією, серед трьох основних ризиків, які в даний час пов'язані з банківською справою в мережі Internet, саме мобільний банкінг перебуває на першому місці.

Перелічені фактори зумовлюють актуальність розробки методів і засобів генерації криптоключів високої криптостійкості для систем клієнт-банк з орієнтацією саме на мобільний банкінг.

Формування криптоключів системи клієнт-банк базується на використанні псевдовипадкових чисел та засобів їх генерації, при чому генерація якісної випадкової послідовності чисел – найскладніша частина багатьох криптографічних операцій [6–9].

Стрімке вторгнення на ринок банківських послуг мобільного банкінгу створює не лише нові загрози, але і нові можливості. Зокрема, в [10, 11] описується технологія застосування датчиків мобільних пристроїв в якості генератора псевдовипадкових чисел. Аналіз специфіки роботи датчиків мобільних пристроїв, характерна змінюваність складу датчиків між моделями та різна їх продуктивність – сукупність факторів, які не дозволяють розглядати зазначені датчики як стабільні і високопродуктивні генератори криптоключів системи клієнт-банк [12]. В той же час, в [12] висунуто гіпотезу про перспективність використання цих датчиків в якості ефективних джерел первинної ентропії, для підтвердження якої запропоновано математичну і узагальнену структурну моделі процесу генерації псевдовипадкових чисел підвищеної ентропії.

Запропоновані в [12] моделі процесу генерації псевдовипадкових чисел містять інструментарій і опис загальних підходів для реалізації генератора криптоключів з джерелами ентропії у вигляді датчиків мобільного пристрою для системи клієнт-банк при наданні послуг мобільного банкінгу, але вони потребують подальшої деталізації і уточнення з метою практичного застосування, що і є предметом даної роботи.

Викладення основного матеріалу

Проведений в [11–13] аналіз свідчить на користь використання датчиків сучасних пристроїв мобільного зв'язку (ПМЗ) в якості джерел первинної ентропії для генераторів криптоключів системи клієнт-банк (при реалізації мобільного банкінгу тощо). В той же час, специфічні особливості різних видів ПМЗ і їх датчиків зумовлюють і специфічні вимоги щодо їх застосування за призначенням.

Серед специфічних властивостей ПМЗ, які мають враховуватися при визначенні положень алгоритму роботи генератора криптоключів підвищеної ентропії, слід відзначити:

- різний набір датчиків у різних видів і моделей ПМЗ;
- різні формати видачі результатів вимірювань і кількість формованих показників для різних датчиків;
- обмежену розрядність результатів вимірювань;
- можливість використання в якості носіїв первинної ентропії лише фрагменту від вектора показника датчика.

Перелічені властивості ПМЗ і їх датчиків обмежують можливості зазначених датчиків щодо генерації векторів-носіїв ентропії з розрядністю, відповідною потребам завдань генерації криптоключів високої криптостійкості. Таким чином, актуальною стає задача накопичення множини або, іншими термінами, пулу значень векторів-носіїв ентропії з загальною розрядністю, достатньою для забезпечення криптостійкості систем, які будуть використовувати цей пул.

З наведеної в [12] моделі можна побачити, що відповідна операція підпадає під завдання функції накопичення-поєднання векторів ентропії F_3. Стосовно функції F_3 зазначимо, що вона займає проміжне місце між функціями перетворення двійкових кодів F_2 і F_4 та є залежною від них, тому має бути узгодженою з ними. Функції F_2 виділяє ентропійну складову з векторів-носіїв ентропії $q_{ji} \in Q_{дж.j}$ (де $Q_{дж.j}$ – множина представлених в цифровому вигляді векторів вихідних значень з j-го датчика ПМЗ, використаного в якості джерела ентропії), але не забезпечує достатньої розрядності результуючого вектора. Функція F_3 має поєднати ентропійну складову декількох векторів $q_{ji} \in Q_{дж.j}$ в одному векторі для реалізації функції F_4, яка, в свою чергу, має передати сумарну ентропійну складову «збірного» вектора на вхід криптографічного алгоритму генерації псевдовипадкових значень в заданій розрядності, тобто, виконати стиснення вектора до потрібної розрядності без втрат ентропійних властивостей. В [12] було також рекомендовано тип функції F_4 як хеш-функції, але не визначено вимог до неї.

В системах клієнт-банк, як правило, використовуються функції хешування розрядністю 256 біт, які визнані достатньо захищеними і криптостійкими для виконання покладених на них завдань.

В поширеній сьогодні системі клієнт-банк «iBank 2 UA» використовується процедура обчислення хеш-функції ГОСТ Р34.11-94, яка видає хеш-функції розрядністю 256 біт. Довжина хеш-функції щонайменше в 256 біт для криптографічних задач обирається для того, щоб забезпечити стійкість до атак із застосуванням сучасних обчислювальних технологій. Довжина 64 біти визнана занадто малою в сучасних умовах, а довжина 128 біт – ризикованою для гарантованого захисту. Стосовно процедури обчислення хеш-функції ГОСТ Р34.11-94 слід зазначити, що на сьогодні ця розробка 1994 року минулого сторіччя визнана вже застарілою і, крім того, є інструментом криптозахисту від країни-агресора, що робить її використання в нашому дослідженні як обов'язкового компонента необґрунтованим.

Більш якісною альтернативою хеш-функції ГОСТ Р34.11-94 є визнаний у всьому світі стандарт SHA-256 (Secure Hash Algorithm) – криптографічна хеш-функція, розрядність якої на виході дорівнює 256 біт, вперше розроблена Агентством національної безпеки США навесні 2002 року і належить до хеш-функцій класу SHA-2, ключі якого до сьогодні не скомпрометовані. [14]

Оскільки алгоритм хеш-функції SHA-256 може бути рекомендований, але не є стандартом хешування в системі клієнт-банк України, в подальшому дослідженні будемо оперувати узагальненим поняттям хеш-функції H256, яке може бути застосоване до хеш-функції SHA-256, до хеш-функції ГОСТ Р34.11-94, а також до ряду існуючих і перспективних функцій.

Головним висновком з проведеного аналізу є те, що функція F_4 запропонованої математичної моделі є підвидом хеш-функції H256, тобто, має розрядність R=256 біт. З цього слідує висновок, що для реалізації алгоритму роботи системи клієнт-банк із застосуванням генераторів криптоключів підвищеної ентропії, згідно із запропонованими принципами, необхідно мати пул ентропії розрядністю щонайменше 256 біт. Цей пул має бути отриманий від будь-якого набору датчиків у різних видів і моделей ПМЗ з урахуванням можливості використання в якості носіїв первинної ентропії фрагменту значення показника датчика.

Для алгоритмічного опису процедури формування і обробки пулу ентропії від датчиків ПМЗ введемо математичний опис операції визначення розрядності $r_{j.i}$ векторів $q_{ji} \in Q_{дж.j}$:

$$r_{ji} = |q_{ji}|. \quad (1)$$

При використанні в якості джерел ентропії n датчиків сумарна розрядність пулу ентропії ΔR, генерованого функцією F_3 при однократному опитуванні датчиків, буде визначатись як сумарна розрядність всіх отримуваних з виходу функції F_2 векторів-носіїв ентропії $q_{ji} \in Q_{дж.j}$:

$$\Delta R = \sum_{i=1}^{n} r_{ji} \quad . \quad (2)$$

Мінімально-достатня кількість ітерацій K однократного одержання пулу векторів-носіїв від всіх джерел для формування загального пулу розрядністю R може бути розрахована за формулою:

$$K = R/\Delta R. \quad (3)$$

За K ітерацій необхідний пул має бути сформований, що є підставою для виконання функцій хешування F_4 і функції генерації ключів підвищеної ентропії F_5 за характерними для них типовими алгоритмами.

За потреби розмір пулу може бути збільшений, але це збільшить час на формування вибірки.

З урахуванням висновків, зроблених при визначенні методології накопичення і обробки пулу ентропії, запропоновану в [12] модель процесу генерації псевдовипадкових чисел, відображену трьохрівневою структурою послідовно-виконуваних операцій F_1-F_5 доцільно уточнити з урахуванням специфічних особливостей застосування датчиків ПМЗ в якості джерел первинної ентропії.

Для доведення моделі у відповідність положенням запропонованої методики накопичення і обробки пулу ентропії необхідно врахувати потребу адаптованості пропонованого методу до кількості наявних в ПМЗ датчиків-джерел ентропії. Зазначена операція, з однієї сторони, є невід'ємною складовою алгоритму роботи з датчиками ПМЗ, а з іншої сторони, не відноситься до числа операції, які безпосередньо забезпечують перетворення сигналів і даних, що несуть ентропію шумових явищ від наявних джерел ентропії.

Виходячи з останнього твердження, адаптацію генератора до кількості наявних в ПМЗ датчиків-джерел ентропії можна ідентифікувати як підготовчу операцію алгоритму роботи системи, тому позначимо її як підготовчу операцію F_0 (рис.1).

На підставі проведеного аналізу і зроблених висновків уточнимо перелік базових функцій алгоритму генерації криптоключів для системи клієнт-банк із застосуванням датчиків мобільних пристроїв як джерел ентропії:

- F_0 – функція-процедура визначення кількості датчиків-джерел ентропії та їх ідентифікації;
- F_1 – функція-процедура зчитування даних показників датчиків (перетворення аналогового сигналу (сигналів) в вектор (вектори) цифрового коду з допомогою датчиків ПМЗ);
- F_2 – функція-процедура виділення з вектора (векторів) показників датчиків розрядів, що несуть максимальну ентропійну складову;

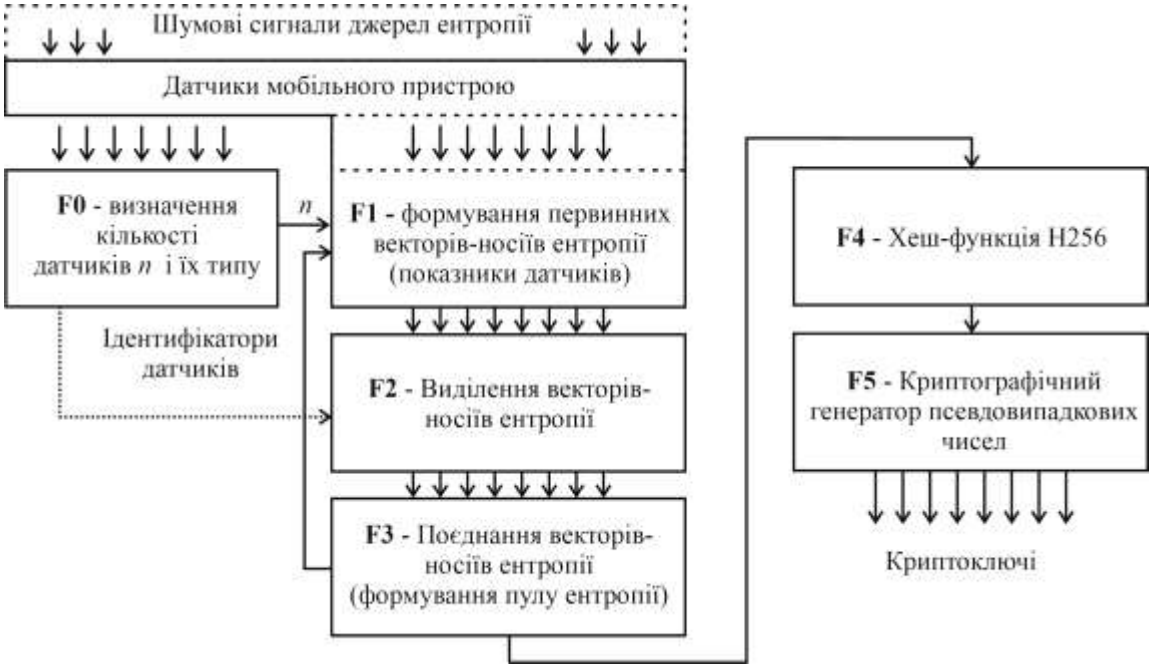

Рис.1. Деталізована функціональна модель процесу генерації криптоключів із застосуванням датчиків мобільних пристроїв в якості джерел ентропії

- F_3 – функція-процедура накопичення пулу ентропії і формування вигляді єдиного вектора-носія ентропії заданої розрядності;
- F_4 – функція-процедура хешування вектора-носія ентропії;
- F_5 – функція-процедура криптографічного методу генерації псевдовипадкових чисел.

Виконання перелічених функцій має забезпечити формування послідовностей псевдовипадкових чисел з максимальним збереженням ентропійних властивостей, отримуваних від джерел ентропії, що дозволяє ідентифікувати отримувані послідовності чисел як випадкові, а побудований за наведеними принципами генератори розглядати як генератори криптоключів підвищеної ентропії.

Висновки

В роботі деталізовано базові принципи використання датчиків пристроїв мобільного зв'язку в якості джерел первинної ентропії генераторів криптоключів системи клієнт-банк при наданні послуг мобільного банкінгу, сформовано обґрунтований опис процедури накопичення і обробки пулу ентропії для реалізації алгоритму роботи системи клієнт-банк із застосуванням генераторів криптоключів підвищеної ентропії, уточнено основні функції процедури та приведено деталізовану функціональну модель процесу генерації криптоключів. Підводячи підсумок проведеним дослідженням з визначення і деталізації базових принципів використання датчиків мобільних пристрої як джерел первинної ентропії, з урахуванням сформульованих правил накопичення і обробки пулу ентропії та використанням інструментарію запропонованої математичної моделі, отримані результати дають можливість виконати деталізацію алгоритму роботи системи клієнт-банк із застосуванням генераторів криптоключів підвищеної ентропії в мобільному банкінгу та інших сервісах.

Література

1. Безпека Інтернет-банкінгу в Україні: практичні аспекти [Електронний ресурс]. – Режим доступу : https://bankchart.com.ua/e_banking/statti/bezpeka_internet_bankingu_v_ukrayini_praktichni_aspekti.

2. Геселева Н.В. Інформаційна система підтримки електронних платежів через Інтернет / Н.В. Геселева, Г.В. Пронюк, В.В. Добровольський // Економіка і суспільство, 2018. – Випуск №14. – С. 1005–1010.

3. Умови надання банківських послуг з використанням систем дистанційного обслуговування [Електронний ресурс]. – Режим доступу : https://www.bisbank.com.ua/wp-content/uploads/2020/08/dodatok-7-umovy_system_dist_obslugov_z–11.05.2019-do-05.07.2019.pdf

4. Система «iBank 2» для корпоративних клієнтів [Електронний ресурс]. – Режим доступу : https://ibank.otpbank.ru/Corporate_Internet–Banking_Guide.pdf.

5. Khatri P. The importance of cyber security in banking [Електронний ресурс] / Prem Khatri: Vice President of Operations, Chetu, Inc. – The Global Treasurer, Categories: Banking Cyber Security & Fraud Technology. – September 25, 2019.– Режим доступу : https://www.theglobaltreasurer.com/2019/09/25/the-importance-of-cyber-security-in-banking/.

6. Горицький В.М. Генерація випадкових послідовностей для систем управління ключами / В.М. Горицький, О.В. Снєжок, М.С. Височіненко // Сучасний захист інформації, 2012. – № 4. – С. 88–95.

6. Гріненко Т. О. Квантові генератори випадкових чисел в криптографії / Т. О. Гріненко, О. П. Нарєжній // Системи обробки інформації. – 2015. – Вип. 10. – С. 86–89.

7. Heat transfer and entropy generation in a microchannel with longitudinal vortex generators using nanofluids / Amin Ebrahimia, Farhad Rikhtegarb, Amin Sabaghana, Ehsan Roohia Energy // Energy. – Volume 101, 15 April 2016. – P. 190–201.

8. Фауре Е. В. Синтез і аналіз псевдовипадкових послідовностей на основі операцій криптографічного перетворення / Е. В. Фауре, С. В. Сисоєнко, Т. В. Миронюк // Системи управління, навігації та зв'язку. – 2015. – Вип. 4. – С. 85–87.

9. Toward sensorbased random number generation for mobile and IoT devices / K. Wallace, K. Moran, E. Novak, G. Zhou, K. Sun // IEEE Internet Things J. – Dec. 2016. – Vol. 3, № 6. – P. 1189–1201.

10. Демський О.О. Метод реалізації генератора випадкових чисел / О.О. Демський, В.О. Бойчук // «Інтелектуальний потенціал – 2018» : збірник наукових праць молодих науковців і студентів з нагоди 30-річчя підготовки ІТ-фахівців в ХНУ. – Хмельницький : ПВНЗ УЕП, 2018. – Ч. 3: Кібербезпека та актуальні проблеми комп'ютерних систем і мереж. – С. 40–44.

11. Модель генератора криптоключів з джерелами ентропії для системи клієнт-банк / В. С. Орленко, В. М. Чешун, О. С. Андрощук, А. І. Катаєва // Міжнародний науково-технічний журнал «Вимірювальна та обчислювальна техніка в технологічних процесах» – 2020. – № 2. – С. 103–112.

12. Чешун В. М. Оцінка ефективності роботи генератора криптоключів підвищеної ентропії для системи клієнт–банк / В. М. Чешун, В. І. Чорненький, В. В. Яцків // Збірник наукових праць молодих науковців і студентів «Інтелектуальний потенціал – 2020». – Хмельницький : ПВНЗ УЕП, 2020. – Частина 2. – С. 84–93.

13. Lane Wagner, How SHA-2 Works Step-By-Step (SHA-256) / Published July 8, 2020 [Електронний ресурс]. – Режим доступу : https://qvault.io/2020/07/08/how-sha-2-works-step-by-step-sha-256.

References

1. Bezpeka Internet–bankinghu v Ukrajini: praktychni aspekty [Elektronnyj resurs]. – URL: https://bankchart.com.ua/e_banking/statti/bezpeka_internet_bankingu_v_ukrayini_praktichni_aspekti.

2. Gheseleva N.V. Informacijna systema pidtrymky elektronnykh platezhiv cherez Internet / N.V. Gheseleva, Gh.V. Pronjuk, V.V. Dobrovoljsjkyj// Ekonomika i suspiljstvo, 2018. – Vypusk #14. – S. 1005–1010.

3. Umovy nadannja bankivsjkykh poslugh z vykorystannjam system dystancijnogho obslughovuvannja [Elektronnyj resurs]. – URL: https://www.bisbank.com.ua/wp-content/uploads/2020/08/dodatok-7-umovy_system_dist_obslugov_z–11.05.2019-do-05.07.2019.pdf

4. Systema «iBank 2» dlja korporatyvnykh klijentiv. [Elektronnyj resurs]. – URL: https://ibank.otpbank.ru/Corporate_Internet–Banking_Guide.pdf.

5. Khatri P. The importance of cyber security in banking [Elektronnyj resurs]. / Prem Khatri: Vice President of Operations, Chetu, Inc. – The Global Treasurer, Categories: Banking Cyber Security & Fraud Technology. – September 25, 2019. – URL: https://www.theglobaltreasurer.com/2019/09/25/the-importance-of-cyber-security-in-banking/.

6. Ghorycjkyj V.M. Gheneracija vypadkovykh poslidovnostej dlja system upravlinnja kljuchamy / V.M. Ghorycjkyj, O.V. Snjezhok, M.S. Vysochinenko // Suchasnyj zakhyst informaciji, 2012. – #4. – S. 88–95.

7. Ghrinenko T. O. Kvantovi gheneratory vypadkovykh chysel v kryptoghrafiji / T. O. Ghrinenko, O. P. Narjezhnij // Systemy obrobky informaciji. – 2015. ¬– Vyp. 10. – S. 86–89.

8. Heat transfer and entropy generation in a microchannel with longitudinal vortex generators using nanofluids / Amin Ebrahimia, Farhad Rikhtegarb, Amin Sabaghana, Ehsan Roohia Energy // Energy. – Volume 101, 15 April 2016. – P. 190–201.

9. Faure E. V. Syntez i analiz psevdovypadkovykh poslidovnostej na osnovi operacij kryptoghrafichnogho peretvorennja / E. V. Faure, S. V. Sysojenko, T. V. Myronjuk // Systemy upravlinnja, navighaciji ta zv'jazku. – 2015. – Vyp. 4. – S. 85–87.

10. Toward sensorbased random number generation for mobile and IoT devices / K. Wallace, K. Moran, E. Novak, G. Zhou, K. Sun //IEEE Internet Things J. – Dec. 2016. – Vol. 3, # 6. – P. 1189–1201.

11. Demskyi O.O. Metod realizatsii heneratora vypadkovykh chysel / O.O. Demskyi, V.O. Boichuk // «Intelektualnyi potentsial – 2018» - zbirnyk naukovykh prats molodykh naukovtsiv i studentiv z nahody 30-richchia pidhotovky IT- fakhivtsiv v KhNU. – Khmelnytskyi: PVNZ UEP, 2018. – Ch.3: Kiberbezpeka ta aktualni problemy kompiuternykh system i merezh. – S. 40–44 .

12. Modelj gheneratora kryptokljuchiv z dzherelamy entropiji dlja systemy klijent-bank / V. S. Orlenko, V. M. Cheshun, O. S. Androshhuk, A. I. Katajeva // Mizhnarodnyj naukovo-tekhnichnyj zhurnal «Vymirjuvaljna ta obchysljuvaljna tekhnika v tekhnologhichnykh procesakh» – 2020. – # 2. – S. 103–112.

13. Cheshun V. M. Ocinka efektyvnosti roboty gheneratora kryptokljuchiv pidvyshhenoji entropiji dlja systemy klijent–bank / V. M. Cheshun, V. I. Chornenjkyj, V. V. Jackiv // Zbirnyk naukovykh pracj molodykh naukovciv i studentiv «Intelektualjnyj potencial – 2020». – Khmeljnycjkyj: PVNZ UEP, 2020. – Chastyna 2. – S. 84–93.

14. Lane Wagner, How SHA-2 Works Step-By-Step (SHA-256) / Published July 8, 2020. [Elektronnyj resurs]. – URL: https://qvault.io/2020/07/08/how-sha-2-works-step-by-step-sha-256.

Рецензія/Peer review : 07.01.2021 р. Надрукована/Printed : 10.03.2021 р.