УДК 004.056.55

С.И. Разенков, В.Н. Борщь

Интеграция отечественного шифрования в протокол PDCP сетей связи пятого поколения

Набор стандартных алгоритмов шифрования Packet Data Convergence Protocol (PDCP) сетей пятого поколения предлагается дополнить ГОСТ Р 34.12–2015 («Кузнечик»). Описывается создание программной библиотеки высокопроизводительных реализаций алгоритмов шифрования для применения в PDCP, протоколе второго уровня сетей связи пятого поколения. Особое внимание уделено оптимизации программных компонент с использованием низкоуровневых процессорных инструкций архитектуры x86: AES-NI и AVX. Представлены результаты для двух наиболее распространенных и надежных алгоритмов: AES и «Кузнечик». В рамках исследования проводилась потактовая оценка эффективности реализованных алгоритмов и сравнение их производительности. Также представлено описание произведенных оптимизаций и путей дальнейшего развития и повышения производительности алгоритма «Кузнечик» для применения в PDCP.
Ключевые слова: 5GNR, 3GPP, PDCP, шифрование, «Кузнечик», AES, системы связи.
DOI: 10.21293/1818-0442-2024-27-1-44-48

Целью работы является исследование возможности интеграции отечественного алгоритма шифрования «Кузнечик» в современные сети связи и оценка производительности такого решения.

Сети пятого поколения получают все большее распространение, стандартный стек протоколов находит свое применение не только в наземных, но и в non-terrestrial networks (NTN, неназемные сети) [1]. Также актуальность обусловлена необходимостью использования отечественных средств криптографической защиты информации для защиты сетей связи согласно стратегии развития отрасли связи РФ на период до 2035 г. [2].

Операции по зашифрованию и расшифрованию пользовательского трафика реализованы на канальном уровне, в PDCP [3]. Всего стандартом описываются 4 режима работы шифрования в PDCP [4]: шифрование выключено, алгоритмы на основе SNOW 3G, ZUC, AES.

Шифры SNOW 3G и ZUC имеют относительно низкую степень защиты и применяются, в основном, для обеспечения обратной совместимости с предыдущими поколениями сетей связи [5], поэтому их развитие и оптимизация не рассматриваются в данной работе. Несмотря на это, указанные шифры также реализованы в библиотеке для полной поддержки стандарта.

Наиболее распространенным и эффективным является алгоритм AES. В том числе алгоритм поддерживается на аппаратном уровне в архитектуре процессоров x86 и ARM: набор инструкций AES-NI.

В работе предлагается дополнить набор шифров PDCP шифром ГОСТ Р 34.12–2015 «Кузнечик», который обеспечивает схожую или лучшую защищенность по сравнению с AES [6]. Из-за меньшего распространения и относительной новизны шифр не имеет аппаратной поддержки в архитектурах современных процессоров.

Для получения максимальной производительности библиотека алгоритмов шифрования реализовывается на языке C. В том числе используется набор инструкций AES-NI для шифра AES. Для шифра «Кузнечик» в работе проводится оптимизация для достижения максимальной производительности в рамках архитектуры x86: применяется набор инструкций для векторных вычислений AVX.

Сравнение алгоритмов проводится через потактовое измерение производительности шифров.

Описание PDCP

PDCP является сетевым протоколом 2-го уровня (канальный уровень), предоставляющим протоколам более высокого уровня, в частности RRC (Radio Resource Control) [7], следующий функционал:

– передача информации (управляющей и пользовательской);

– обслуживание порядковых номеров (PDCP SNs);

– сжатие и распаковка заголовков с помощью протокола ROHC;

– сжатие и распаковка заголовков с помощью протокола EHC;

– сжатие и распаковка исходящих данных с помощью протокола UDC;

– зашифрование и расшифрование;

– защита и проверка целостности;

– отбрасывание пакетов SDU по таймеру;

– маршрутизация (для DAPS- и split-соединений);

– дублирование;

– упорядочивание входящих пакетов;

– отбрасывание дублирующих входящих пакетов.

В свою очередь, сущность протокола PDCP связана с множеством сущностей RLC (Radio Link control), другого протокола 2-го уровня.

В данной работе рассматривается только функционал, относящийся к задаче шифрования.

Шифрование в PDCP

В PDCP каждому алгоритму шифрования соответствует 4-битный идентификатор:

– 0000 – NEA0 нулевой алгоритм (отключение шифрования);

– 0001 – 128-NEA1 128-битный алгоритм на основе SNOW 3G;

– 0010 – 128-NEA2 128-битный алгоритм на основе AES;

– 0011 – 128-NEA3 128-битный алгоритм на основе ZUC.

Каждый алгоритм шифрования принимает следующие исходные данные:

– 128-битный ключ KEY;

– 32-битное значение параметра COUNT;

– 5-битный идентификатор соединения BEARER;

– 1-битное значение направления соединения DIRECTION (0 для восходящей линии и 1 для нисходящей);

– длина LENGTH требуемой ключевой последовательности (гаммы).

Порядок использования шифрсистемы NEA при зашифровании открытого текста следующий (рис. 1): генерируемый блок гаммы KEYSTREAM побитно складывается по модулю 2 с блоком открытого текста PLAINTEXT. Расшифрование происходит аналогичным образом: генерируется блок гаммы KEYSTREAM с использованием тех же входных параметров и происходит ее наложение на блок шифртекста CIPHERTEXT.

Входной параметр LENGTH должен влиять только на длину блока KEYSTREAM, но не на значения бит в нем.

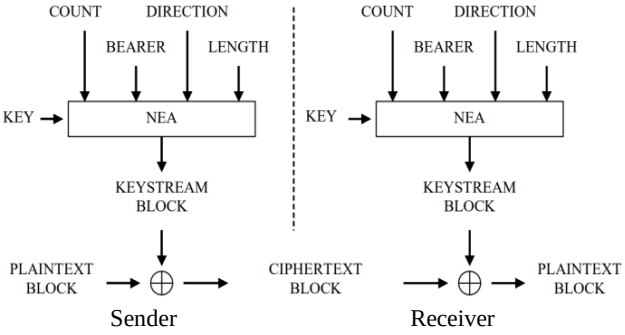

Рис. 1. Схема шифрования в PDCP

Представленная схема позволяет заменить шифр любым подходящим, работающим в режиме гаммирования.

Алгоритм 128-NEA2, AES

В этом режиме зашифрование и расшифрование данных выполняется с помощью AES-128 [8] в режиме CTR [9] (счетчика). Шифр AES-128 является 128-битным блочным шифром и состоит из 10 раундов, включающих нелинейное преобразование, выполняемое согласно таблице подстановок, циклические сдвиги последних трех четверок байт на 3, 2 и 1 байт, начиная назад с последнего, умножение на фиксированный полином $a(x) = 3x^3 + x^2 + x + 2$ в поле Галуа по модулю полинома $x^4 + 1$ и побитное сложение по модулю 2 с раундовым ключом, получаемым из ключа шифрования по специальной процедуре.

Режим CTR заключается в формировании последовательности 128-битных блоков счетчика T_1, T_2, ..., T_i, независимо друг от друга шифруемых с помощью AES, а затем побитно складываемых с данными по модулю 2.

Последовательность блоков счетчика формируется следующим образом: 64 старших бит T_1 равны COUNT| BEARER | DIRECTION | 0^{26} (26 нулевых бит). Младшие 64 бит T_1 равны 0. Последующие блоки T_i получаются в результате инкрементирования младших 64 бит T_{i-1} по модулю 2^{64} [10].

Алгоритм 256-NEA4, «Кузнечик»

Для поддержки отечественного алгоритма шифрования ГОСТ Р 34.12–2015 («Кузнечик») [11] в PDCP был внедрен дополнительный режим работы 256-NEA4(идентификатор 0100), использующий данный шифр в режиме CTR, где инициализация счетчика происходит аналогично 128-NEA2.

«Кузнечик» является 128-битным блочным шифром с размером ключа шифрования 256 бит. Шифр состоит из 9 раундов, в которых выполняется побитовое сложение по модулю 2 с раундовым ключом, нелинейное биективное преобразование и линейное преобразование, а также 10-го раунда, содержащего только побитное сложение по модулю 2 с раундовым ключом.

В PDCP для алгоритма шифрования NEA есть возможность использовать ключ KEY длиной до 256 бит включительно, так как он является результатом усечения 256-битного выходного значения функции KDF (Key Derivation Function) [4]. Это позволяет внедрить «Кузнечик» в протокол PDCP.

Программная реализация

При реализации режимов 128-NEA1 и 128-NEA3 были использованы программный код шифров Snow 3G и ZUC и тестовые последовательности из соответствующих спецификаций [12,13].

Для режима 128-NEA2 была использована реализация AES из [14]. Эта реализация была оптимизирована с использованием инструкций AES-NI, расширения системы команд архитектуры x86, созданного с целью ускорения криптографических операций AES на процессорах архитектуры x86. Код этой реализации частично заимствован из [15]. При проверке реализаций на корректность были использованы тестовые последовательности из [10].

Для получения общего представления о работе алгоритма и эталонных значений производительности при прямом переносе алгоритма в код была использована готовая реализация «Кузнечика» из [16]. Полученные результаты (таблица) показали низкую производительность «Кузнечика» по сравнению с AES.

Пропускная способность криптографических алгоритмов (Гбит/с)

Шифр	Реализация	Размер блоков (общий размер 1 МБ)		
		64 Б	1 КБ	8 КБ
AES	Без оптимизации	0,388	0,729	0,768
	AES-NI	0,757	5,246	7,681
Кузнечик	Без оптимизации	0,005	0,012	0,013
	Оптимизированная	0,316	1,351	1,697

Проведена оптимизация реализации шифра «Кузнечик». При создании оптимизированной реализации за основу взято описание из [17]. Повышение производительности достигается за счет исполь-

зования векторных инструкций процессора, а также таблиц предвычислений.

Использование 256-битных векторных регистров из набора инструкций AVX2 позволяет проводить побитовое сложение двух блоков по модулю 2 с раундовыми ключами за одну инструкцию.

Таблица предвычислений хранит результаты выполнения двух операций – нелинейного биективного и линейного преобразований. Таким образом, чтобы выполнить эти два преобразования, нужно извлечь соответствующее значение из таблицы предвычислений, что гораздо быстрее, чем прямой расчет. Инициализация таблиц предвычислений не зависит от шифруемых данных и значения ключа, поэтому может осуществляться однократно перед работой с функцией шифрования. Данное изменение позволило в 5–6 раз увеличить среднюю скорость шифрования данных.

Экспериментальные результаты

Измерения задержки и пропускной способности [18] проводились с использованием процессора Intel (R) Core (TM) i7-8700KCPU @ 3.7 GHz. Измерения проводились в обычном режиме работы процессора, без изоляции ядра, ОС Ubuntu 22.04 без графической оболочки. Тестовое приложение привязано к одному ядру инструкцией processor affinity.

Оценка производительности библиотеки проводилась следующим образом:

1. Подготовка массива случайных данных суммарным размером 1 МБ и разбитым на блоки определенного размера: 64 Б, 1 кБ, 8 кБ.

2. Зашифрование/расшифрование блоков данных с измерением количества тактов ЦПУ, затраченных на операцию.

3. Пункт 2 выполняется 1 024 раза, затраченное на обработку количество тактов ЦПУ сохраняется.

Такой подход позволяет оценить производительность алгоритмов без привязки к тактовой частоте процессора. Измерение производительности в тактах позволяет вычислить задержку для процессоров с такой же микроархитектурой (Intel Coffee Lake) с высокой точностью и с меньшей точностью для процессоров со схожими микроархитектурами.

В таблице представлена пропускная способность реализаций алгоритмов AES и «Кузнечик» за 1 024 итерации обработки случайных данных размером 1 МБ и разбитых на блоки для выбранного процессора.

На рис. 2 изображены графики тактов процессора при обработке блоков размером 1 кБ. Для других размеров блоков характер графиков повторяется.

Заключение

Разработана библиотека алгоритмов шифрования для протокола PDCP сетей 5G NR.

В качестве альтернативы наиболее популярному алгоритму шифрования AES предложен ГОСТ Р 34.12–2015 «Кузнечик», обеспечивающий схожую стойкость.

Представлены оптимизированные версии наиболее широко используемых алгоритмов: AES и «Кузнечик».

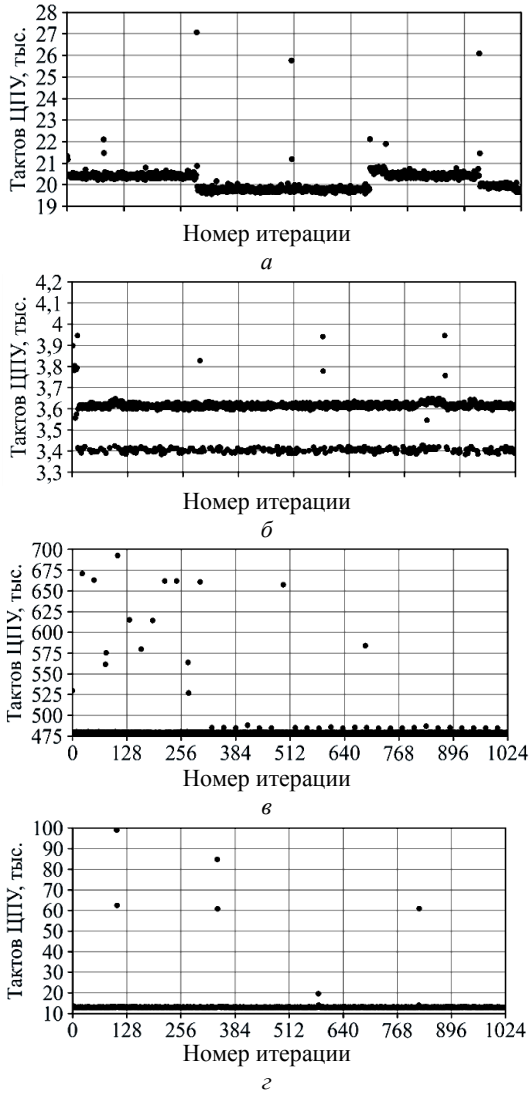

Рис. 2. Длительность работы алгоритма: 128-NEA1 – *а*, 128-NEA2 – *б*, 128-NEA3 – *в*, 256-NEA4 – *г*

Для обоих алгоритмов проведено потактовое измерение производительности, которое демонстрирует низкую величину джиттера (jitter) работы алгоритмов. Для шифра AES эта величина составляет около 1 000 тактов, для «Кузнечика» – около 6 000 тактов.

«Выбросы» на рис. 4 являются отклонениями от среднего числа затрачиваемых процессором тактов, вызванными переключением процессора на другие задачи и/или переносом контекста между ядрами. При необходимости снижения уровня джиттера возможно переключение ядра ЦПУ в изолированный режим. Общее количество таких «выбросов» незначительно, однако их вкладом в джиттер нельзя пренебрегать.

Разработанное программное решение может применяться для закрытия каналов данных до 1 Гбит/с при невысоких требованиях к аппаратной платформе. Библиотека имеет стандартный API для интеграции с имеющимся стеком PDCP.

Шифр AES в силу наличия расширенного набора инструкций в процессорах архитектуры x86 име-

ет наибольшую производительность и значительно превосходит шифр «Кузнечик». Проведенные оптимизации: использование векторных инструкций, таблиц предвычислений и итерационных констант – ускорили работу шифра «Кузнечик». Получена производительность на уровне 20% от производительности AES.

Полученные результаты демонстрируют несостоятельность идеи применения программной реализации шифра «Кузнечик» для высокопроизводительных систем связи. Поэтому перспективным развитием реализации шифра «Кузнечик» будет использование аппаратного ускорителя (на базе ПЛИС) или расширение аппаратного набора инструкций современных процессоров с открытой архитектурой, такой как RISC-V.

Литература

1. 3GPP TS 21.915 V17.1.0 [Электронный ресурс]. – Режим доступа: https://www.3gpp.org/ftp/Specs/archive/21_series/21.905/21905-h10.zip, свободный (дата обращения: 06.04.2023).

2. Распоряжение Правительства РФ от 24.11.2023 № 3339-р (вместе со «Стратегией развития отрасли связи Российской Федерации на период до 2035 года») [Электронный ресурс]. – Режим доступа: http://publication.pravo.gov.ru/document/0001202312040015, свободный (дата обращения: 27.12.2023).

3. 3GPP TS 38.323 V17.3.0 [Электронный ресурс]. – Режим доступа: https://www.3gpp.org/ftp/Specs/archive/38_series/38.323/38323-h30.zip, свободный (дата обращения: 03.04.2023).

4. 3GPP TS 33.501 V18.0.0. [Электронный ресурс]. – Режим доступа: https://www.3gpp.org/ftp/Specs/archive/33_series/33.501/33501-i00.zip, свободный (дата обращения: 26.03.2023).

5. Бурмакин А.О. Обзор угроз безопасности сетей стандарта LTE / А.О. Бурмакин, Э.А. Воробьев, В.А. Гохович // Синергия наук. – 2019. – № 38. – С. 127–140.

6. Соболев М.А. Сравнительный анализ российского стандарта шифрования по ГОСТ Р 34.12–2015 и американского стандарта шифрования AES // Политехнический молодежный журнал. – 2022. – № 04(69). – URL: https://ptsj.ru/articles/785/eng/785.pdf, (дата обращения: 07.11.2023).

7. 3GPP TS 38.331 V17.3.0 [Электронный ресурс]. – Режим доступа: https://www.3gpp.org/ftp/Specs/archive/38_series/38.331/38331-h30.zip, свободный (дата обращения: 15.06.2023).

8. National Institute of Standards and Technology. Advanced Encryption Standard (AES) (FIPS PUB 197). – URL: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf, (дата обращения: 26.03.2023).

9. National Institute of Standards and Technology Special Publication 800-38A 2001 ED Natl. Inst. Stand. Technol. Spec. Publ. 800-38A 2001 ED, 66 pages (December 2001. – URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38a.pdf (дата обращения: 26.03.2023).

10. 3GPP TS 33.401 V17.3.0 [Электронный ресурс]. – Режим доступа: https://www.3gpp.org/ftp/Specs/archive/33_series/33.401/33401-h30.zip, свободный (дата обращения: 26.03.2023).

11. ГОСТ Р 34.12–2015. Информационная технология. Криптографическая защита информации. Блочные шифры. – М.: Стандартинформ, 2015. – 21 с.

12. 3GPP TS 35.215 V17.0.0 [Электронный ресурс]. – Режим доступа: https://www.3gpp.org/ftp/Specs/archive/35_series/35.215/35215-h00.zip, свободный (дата обращения: 26.03.2023).

13. 3GPP TS 35.221 V17.0.0 [Электронный ресурс]. – Режим доступа: https://www.3gpp.org/ftp/Specs/archive/35_series/35.221/35221-h00.zip, свободный (дата обращения: 26.03.2023).

14. Tiny AES in C [Электронный ресурс]. – Режим доступа: https://github.com/kokke/tiny-AES-c, свободный (дата обращения: 08.05.2023).

15. Shay Gueron. Mobility Group, Israel Development Center Intel Corporation. «Intel® Advanced Encryption Standard (AES) New Instructions Set». – 2010. – URL: https://www.intel.com/content/dam/doc/white-zaper/advanced-encryption-standard-new-instructions-set-paper.pdf (дата обращения: 10.05.2023).

16. Implementation of the proposed Russian block cipher standard, Kuznechik («Grasshopper»). 128-bit block size, 256-bit key [Электронный ресурс]. – Режим доступа: https://github.com/mjosaarinen/kuznechik, свободный (дата обращения: 12.05.2023).

17. Дорохин С.В. Реализация блочного шифра «Кузнечик» с использованием векторных инструкций / С.В. Дорохин, С.С. Качков, А.А. Сидоренко // Труды МФТИ. – 2018. –Т. 10, № 4 (40). – С. 45–53.

18. BigMac: Performance Overhead of User Plane Integrity Protection in 5G networks / T. Heijligenberg, G. Knips, C. Böhm, D. Rupprecht, K. Kohls // In Proceedings of the 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec ’23). – May 29 – June 1, 2023, Guildford, United Kingdom. – ACM, New York, NY, USA. – 6 p. – URL: https://doi.org/10.1145/3558482.3581777 (дата обращения: 07.11.2023).

Разенков Семен Игоревич
Студент Института прикладной математики
и компьютерных наук (ИПМКН)
Томского государственного университета (ТГУ)
Ленина пр-т, 36, г. Томск, Россия, 634050
Тел.: +7 (382-2) 52-94-96
Эл. почта: sirazenkov@gmail.com

Борщь Владислав Николаевич
Аспирант каф. телекоммуникаций и основ радиотехники
(ТОР) Томского государственного университета
систем управления и радиоэлектроники (ТУСУР)
Ленина пр-т, 40, г. Томск, Россия, 634000
ORCID: 0000-0002-5479-1982
Тел.: +7 (382-2) 41-33-98
Эл. почта: borchsh.vn@gmail.com

Razenkov S.I., Borshch V.N.

Implementation of encryption in the PDCP protocol of 5G NR network

A software library in C language is created which contains a high-performance implementation of encryption algorithms used in PDCP protocol of 5G NR network. The standard set of algorithms is extended with GOST R 34.12–2015 («Kuznyechik»). Performance optimizations are done by using special extensions to x86 architecture instruction set: AES-NI и AVX. Implementation results for the two most common and secure algorithms, AES and «Kuznyechik», are presented.

Their performance was evaluated including consumed clock cycles during execution. All optimizations are described and development prospects of «Kuznyechik» implementation optimizations are given.

Keywords: 5G NR, 3GPP, encryption, «Kuznyechik», AES, communication systems.

DOI: 10.21293/1818-0442-2024-27-1-44-48

References

1. 3GPP TS 21.915 V17.1.0. Available at: https://www.3gpp.org/ftp/Specs/archive/21_series/21.905/21905-h10.zip, free (Accessed: April 6, 2023).

2. Decree of the Government of the Russian Federation N 3339-p dated 24 November 2023 (with the «Communications industry development strategy of Russia up to 2035»). Available at: http://publication.pravo.gov.ru/document/0001202312040015, free (Accessed: December 27, 2023) (In Russ.).

3. 3GPP TS 38.323 V17.3.0. Available at: https://www.3gpp.org/ftp/Specs/archive/38_series/38.323/38323-h30.zip, free (Accessed: April 3, 2023).

4. 3GPP TS 33.501 V18.0.0. Available at: https://www.3gpp.org/ftp/Specs/archive/33_series/33.501/33501-i00.zip, free (Accessed: March 26, 2023).

5. Burmakin A.O., Vorobev E.A., Gokhovich V.A. Overview of LTE security threats. *Synergy of Science*, 2019, no. 38, pp. 127–140 (in Russ.).

6. Sobolev M.A. Comparative analysis of russian GOST R 34.12-2015 encryption standard and american encryption standard AES. Politekhnicheskiy molodezhnyy zhurnal [Politechnical student journal], 2022., no. 04(69). Available at: https://ptsj.ru/articles/785/eng/785.pdf, free (Accessed: November 7, 2023) (in Russ.).

7. 3GPP TS 38.331 V17.3.0. Available at: https://www.3gpp.org/ftp/Specs/archive/38_series/38.331/38331-h30.zip, free (Accessed: June 15, 2023).

8. National Institute of Standards and Technology. Advanced Encryption Standard (AES) (FIPS PUB 197). Available at: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf, free (Accessed: March 26, 2023).

9. National Institute of Standards and Technology Special Publication 800-38A 2001 ED Natl. Inst. Stand. Technol. Spec. Publ. 800-38A 2001 ED, 66 p. (December 2001. Available at: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38a.pdf, free (Accessed: March 26, 2023)

10. 3GPP TS 33.401 V17.3.0. Available at: https://www.3gpp.org/ftp/Specs/archive/33_series/33.401/33401-h30.zip, free (Accessed: March 26, 2023).

11. «Information technology. Cryptographic data security. Block ciphers», GOST R 34.12–2015, Federal Agency on Technical Regulating and Metrology, 2015, 21 p.

12. 3GPP TS 35.215 V17.0.0. Available at: https://www.3gpp.org/ftp/Specs/archive/35_series/35.215/35215-h00.zip, free (Accessed: March 26, 2023).

13. 3GPP TS 35.221 V17.0.0. Available at: https://www.3gpp.org/ftp/Specs/archive/35_series/35.221/35221-h00.zip, free (Accessed: March 26, 2023).

14. Tiny AES in C. Available at: https://github.com/kokke/tiny-AES-c, free (Accessed: May 8, 2023).

15. Shay Gueron. Mobility Group, Israel Development Center Intel Corporation. «Intel® Advanced Encryption Standard (AES) New Instructions Set», 2010. Available at: https://www.intel.com/content/dam/doc/white-зaper/advanced-encryption-standard-new-instructions-set-paper.pdf, free (Accessed: May 10, 2023).

16. Implementation of the proposed Russian block cipher standard, Kuznechik («Grasshopper»). 128-bit block size, 256-bit key. Available at: https://github.com/mjosaarinen/kuznechik, free (Accessed: May 12, 2023).

17. Dorokhin S.V., Kachkov S.S., Sidorenko A.A. Implementation Of «Kuznyechik» Cipher Using Vector Instructions, *Proceedings of MIPT*, 2018, vol. 10, no. 4, P. 45–53 (in Russ.).

18. Heijligenberg T., Knips G., Böhm C., Rupprecht D., Kohls K. BigMac: Performance Overhead of User Plane Integrity Protection in 5G networks. In Proceedings of the 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '23), May 29 – June 1, 2023, Guildford, United Kingdom. ACM, New York, NY, USA, 6 p. Available at: https://doi.org/10.1145/3558482.3581777, free (Accessed: November 7, 2023).

Semyon I. Razenkov
Graduate student, Computer Security Department,
Institute of Applied Mathematics and Computer Science (IPMC), National Research Tomsk State University (TSU)
36, Lenin pr., Tomsk, Russia, 634050
Phone: +7 (382-2) 52-94-96
Email: sirazenkov@gmail.com

Vladislav N. Borshch
Graduate student, Department of Telecommunications and Basic Principles of Radio Engineering, Tomsk State University of Control Systems and Radioelectronics (TUSUR)
40, Lenin pr., Tomsk, Russia, 634000
ORCID: 0000-0002-5479-1982
Phone: +7 (382-2) 41-33-98
Email: borchsh.vn@gmail.com