

УДК 621.391

© А. А. Гавришев, Д. Л. Осипов, 2023

ПОСТРОЕНИЕ ОБОБЩЕННОГО КРИТЕРИЯ ОЦЕНКИ КАЧЕСТВА КРИПТОСТОЙКИХ КОДОВЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ, ИСПОЛЪЗУЕМЫХ В ЗАЩИЩЕННЫХ БЕСПРОВОДНЫХ СИСТЕМАХ СВЯЗИ

Проведен анализ статистических методов оценки криптостойкости кодовых последовательностей, используемых в защищенных беспроводных системах связи, который показал, что в известных работах не предложен универсальный показатель качества (ПК) оценки криптостойкости кодовых последовательностей. Отмечено, что в качестве ПК для оценки криптостойкости кодовых последовательностей с помощью статистических методов целесообразно сформировать комплекс ПК. В указанный комплекс нужно включить ПК, уже описанные в источниках. Сформированный комплекс ПК, по мнению авторов, позволит более точно оценить криптостойкость кодовых последовательностей, используемых в защищенных беспроводных системах связи. Разработанный комплекс ПК сформирован как единый кортеж, описываемый сформулированным выражением, который может служить обобщенным критерием оценки криптостойкости кодовых последовательностей. Отмечено, что в известных работах в явном виде такой кортеж не представлен. Проведена модернизация описываемого кортежа с учетом ПК, отвечающих за надежность. Установлено, что при использовании в защищенных беспроводных системах связи криптостойких кодовых последовательностей необходимо обращать внимание на этот комплекс ПК. Сформированный обобщенный критерий оценки качества позволит повысить точность оценки криптостойкости кодовых последовательностей при их использовании в защищенных беспроводных системах связи.

Кл. сл.: показатели оценки качества, защищенные беспроводные системы связи, кодовые последовательности, криптостойкость, статистические методы оценки

ВВЕДЕНИЕ

Современные защищенные беспроводные системы связи должны устойчиво функционировать в условиях дестабилизирующих внешних воздействий, например при перехвате третьей стороной передаваемых сигналов или при радиоэлектронном подавлении сигнала. Это обуславливает постоянное совершенствование методов повышения защищенности беспроводных систем связи, позволяющих увеличить уровень априорной неопределенности параметров и характеристик передаваемых сигналов [1–8]. Среди подходов противодействия особо выделяются криптографические методы защиты информации и технологии на основе передачи шумоподобных сигналов (ШПС). При использовании криптографических методов защиты информации или технологий передачи сигналов на основе ШПС важно корректно осуществить выбор качественных кодовых последовательностей, с помощью которых происходит преобразование передаваемой информации к виду, который не сможет прочесть неавторизованный пользователь. Таким образом, задача оценки качества при-

меняемых в защищенных беспроводных системах связи кодовых последовательностей, безусловно, является актуальной.

В настоящее время анализ кодовых последовательностей, применяемых в защищенных беспроводных системах связи, возможно проводить с помощью различных методик. Большинство исследователей полагают, что одним из первичных показателей является криптостойкость кодовых последовательностей, используемых в защищенных беспроводных системах связи [1–8]. Обычно под криптостойкостью кодовых последовательностей понимается их стойкость к нарушению безопасности, которая характеризуется рядом показателей качества (ПК), среди которых часто выделяются следующие [1–8]:

1. На основе известной конечной части кодовой последовательности невозможно определить как ее последующий элемент, так и предыдущий.

2. Неотличимость статистических свойств генерируемых кодовых последовательностей от аналогичных свойств истинно случайной последовательности.

3. Большой период последовательности.

4. Незначительное изменение начальных условий должно приводить к существенному непредсказуемому изменению выходной кодовой последовательности.

Несмотря на то что оценка криптостойкости кодовых последовательностей до сих пор является сложной задачей, такая оценка позволяет выявить возможные дефекты в способе формирования последовательности и оценить приемлемость с точки зрения устойчивости последовательности к раскрытию злоумышленником. Поэтому дальнейшие исследования в указанной области являются важным направлением обеспечения защиты информации, передаваемой с помощью беспроводных систем связи, и требуют дальнейшей проработки [1–8].

Целью данной статьи является повышение точности оценки криптостойкости кодовых последовательностей, используемых в защищенных беспроводных системах связи, за счет применения выявленного обобщенного критерия.

Задачей данной статьи является построение обобщенного критерия оценки качества криптостойких кодовых последовательностей, используемых в защищенных беспроводных системах связи, на основе статистических оценок криптостойкости.

ОСНОВНАЯ ЧАСТЬ

Согласно [1–9], существующие методы оценки криптостойкости кодовых последовательностей, используемых в защищенных беспроводных сис-

темах связи, возможно разделить на две большие группы: аналитические методы и статистические методы.

Аналитические методы позволяют получить характеристики системы как некоторую функцию параметров ее работы. Обычно аналитическая модель представляет совокупность математических выражений и отношений, при решении которых получают параметры, необходимые для оценки исследуемой системы. Часто такими параметрами выступают вероятностные или иные характеристики.

Статистические методы основаны на компьютерном воспроизведении моделей, имитирующих поведение реальных объектов, процессов и систем во времени в течение заданного периода и многократно повторяемых для последующей статистической обработки полученных данных с целью подтверждения их адекватности. С целью упрощения в дальнейших исследованиях акцентируем более подробно внимание на статистических методах оценки криптостойкости кодовых последовательностей. В настоящее время исследователями предложен широкий спектр статистических методов оценки криптостойкости, однако среди них нет универсального ПК — оценки криптостойкости кодовых последовательностей.

В табл. 1 приведены широко распространенные ПК, применяемые в системах связи с ШПС [1–5, 7, 8, 10–14]. С помощью данных ПК проводится оценка криптостойкости кодовых последовательностей, используемых в беспроводных системах связи.

Табл. 1. Примеры ПК, применяемые при оценке криптостойкости кодовых последовательностей с помощью статистических методов оценки, описанные в трудах по системам связи с ШПС

№	ПК кодовых последовательностей	Обозначение	Требование
1	Значение боковых пиков автокорреляционной функции (АКФ)	$R_{A\max}(\tau)$	Кодовые последовательности должны обладать минимальными боковыми пиками АКФ
2	Значение боковых пиков взаимокорреляционной функции (ВКФ)	$R_{C\max}(\tau)$	Кодовые последовательности должны обладать минимальными боковыми пиками ВКФ
3	Количество	Q	Количество кодовых последовательностей должно быть достаточно велико
4	Длина	N	Кодовые последовательности должны обладать максимальной длиной
5	Линейная сложность	L	Кодовые последовательности должны обладать линейной сложностью, равной больше половины длины последовательности

Табл. 2. Примеры ПК, применяемые при оценке криптостойкости кодовых последовательностей с помощью статистических методов оценки, представленных в пакете статистических тестов NIST

№	ПК кодовых последовательностей	Обозначение	Требование
1	Частотный (монобитный тест)	T_1	В кодовых последовательностях число единиц приблизительно должно быть равно числу нулей
2	Блочный тест на частоту	T_2	В кодовых последовательностях количество нулей либо единиц внутри m -битных блоков должно быть примерно одинаковым
3	Тест на серийность	T_3	В кодовых последовательностях должно быть минимальное отклонение числа серий из единиц (из нулей) различной длины, в частности, частоты чередования единиц и нулей
4	Тест на длиннейшую серию единиц в блоке	T_4	В кодовых последовательностях не должно быть отклонения от теоретического закона распределения максимальных длин серий единиц
5	Тест приблизительной энтропии	T_5	Кодовые последовательности не должны иметь свойств регулярности

В более поздних публикациях [7, 15–18] показано, что одним из самых востребованных направлений в области статистических методов оценивания криптостойкости кодовых последовательностей, используемых в защищенных беспроводных системах связи, является применение статистических тестов. Среди них выделяются тесты Д. Кнута, diehard, NIST и др. Из представленных тестов наиболее популярным является пакет статистических тестов (ПСТ) NIST, который находит широкое применение в практической деятельности.

С целью сокращения временных и вычислительных затрат в качестве тестов для оценки криптостойкости кодовых последовательностей, вклю-

ченных в ПСТ NIST, обычно выбираются тесты, представленные в табл. 2 [7, 15–18].

Каждым статистическим тестом, представленным в табл. 2, решается задача проверки гипотезы о криптостойкости входной кодовой последовательности (нулевая гипотеза) либо альтернативная гипотеза (кодовая последовательность не является криптостойкой).

Еще одним инструментарием для оценки криптостойкости кодовых последовательностей, используемых в защищенных беспроводных системах связи, является теория нелинейной динамики [15, 16, 19–23]. В табл. 3 перечислены некоторые из таких ПК.

Табл. 3. Примеры ПК, применяемые при оценке криптостойкости кодовых последовательностей с помощью статистических методов оценки на основе теории нелинейной динамики

№	ПК кодовых последовательностей	Обозначение	Требование
1	Максимальный показатель Ляпунова	$\lambda_{\max}$	Кодовые последовательности должны обладать максимальным положительным показателем Ляпунова
2	Показатель Херста	H	Кодовые последовательности должны обладать показателем Херста, равным 0.5
3	BDS-статистика	$\omega(\varepsilon)$	Кодовые последовательности должны обладать значением BDS-статистики ниже, чем установлено для соответствующего класса кодовых последовательностей

На данный момент ПК, представленные в табл. 3, не нашли широкого применения для оценки криптостойкости кодовых последовательностей. Однако их использование для указанных целей является перспективным, т.к. они позволяют различать структуру кодовых последовательностей и проводить их классификацию.

Проведенный анализ литературы [1–8, 10–23] показывает, что в качестве ПК для оценки криптостойкости кодовых последовательностей с помощью статистических методов оценки криптостойкости целесообразно сформировать комплекс ПК. В указанный комплекс целесообразно включить ПК, описанные в табл. 1–3. Сформированный комплекс ПК, по мнению авторов, позволит более точно оценить криптостойкость кодовых последовательностей, используемых в защищенных беспроводных системах связи. Представленные в табл. 1–3 ПК возможно объединить в единый

кортеж, который может служить обобщенным критерием оценки криптостойкости кодовых последовательностей. Заметим, что в известных работах [1–8, 10–23], в которых исследуются вопросы оценки криптостойкости кодовых последовательностей, используемых в защищенных беспроводных системах связи, в явном виде такой кортеж не представлен.

По аналогии с работой [3] и согласно методическим рекомендациям из работы [24], выпишем содержательную формулировку задачи повышения защищенности функционирования беспроводной системы связи. Для повышения защищенности функционирования беспроводной системы связи при использовании криптостойких кодовых последовательностей необходимо оперировать обобщенным критерием оценки качества таких последовательностей, основанном на статистических оценках и представляющим собой кортеж (1):

$$\langle R_{A\max}(\tau), R_{C\max}(\tau), Q, N, L, T_1, T_2, T_3, T_4, T_5, \lambda_{\max}, H, \omega(\varepsilon) \rangle, \quad (1)$$

в котором:

$$\begin{cases} R_{A\max}(\tau) < R_{A\max\text{ доп}}(\tau), R_{C\max}(\tau) < R_{C\max\text{ доп}}(\tau), Q \rightarrow \max, \\ N \rightarrow \max, L > \frac{N}{2}, T_1 \rightarrow 0.5, T_2 \rightarrow 0.5, T_3 \rightarrow 0.5, T_4 \rightarrow 0.5, \\ T_5 \rightarrow 0.5, \lambda_{\max} \rightarrow \max, H \rightarrow 0.5, \omega(\varepsilon) < \omega_{\text{доп}}(\varepsilon). \end{cases}$$

Здесь $R_{A\max}(\tau)$, $R_{C\max}(\tau)$, Q , N , L — ПК, представленные в табл. 1; T_1, T_2, T_3, T_4, T_5 — ПК по табл. 2; $\lambda_{\max}$, H , $\omega(\varepsilon)$ — ПК по табл. 3; $R_{A\max\text{ доп}}(\tau)$ — допустимое значение боковых пиков АКФ, $R_{C\max\text{ доп}}(\tau)$ — допустимое значение боковых пиков ВКФ, $\omega_{\text{доп}}(\varepsilon)$ — допустимое значение BDS-статистики кодовых последовательностей.

Дополнительно к этому модернизируем представленный кортеж с учетом ПК, отвечающих за надежность [3, 10, 12, 25, 26], в частности, пик-фактора кодовых последовательностей ρ и выбросов их амплитудно-частотных спектров $G(\omega)$, к следующему окончательному виду (2):

$$\langle R_{A\max}(\tau), R_{C\max}(\tau), Q, N, L, T_1, T_2, T_3, T_4, T_5, \lambda_{\max}, H, \omega(\varepsilon), \rho, G(\omega) \rangle, \quad (2)$$

где

$$\begin{cases} R_{A\max}(\tau) < R_{A\max\text{ доп}}(\tau), R_{C\max}(\tau) < R_{C\max\text{ доп}}(\tau), Q \rightarrow \max, \\ N \rightarrow \max, L > \frac{N}{2}, T_1 \rightarrow 0.5, T_2 \rightarrow 0.5, T_3 \rightarrow 0.5, T_4 \rightarrow 0.5, \\ T_5 \rightarrow 0.5, \lambda_{\max} \rightarrow \max, H \rightarrow 0.5, \omega(\varepsilon) < \omega_{\text{доп}}(\varepsilon), \rho < \rho_{\text{доп}}, G(\omega) < G_{\text{доп}}(\omega). \end{cases}$$

Здесь в дополнение к показателям по (1) присутствуют ρ — пик-фактор кодовых последовательностей, $G(\omega)$ — выбросы амплитудно-частотных спектров кодовых последовательностей,

$\rho_{\text{доп}}$ — допустимый пик-фактор кодовых последовательностей, $G_{\text{доп}}(\omega)$ — допустимые выбросы амплитудно-частотных спектров кодовых последовательностей.

ЗАКЛЮЧЕНИЕ

В настоящее время в научной литературе [1–8, 10–23] широко представлены статистические методы оценки криптостойкости кодовых последовательностей, используемые в защищенных беспроводных системах связи. Однако авторами указанных публикаций не предложен универсальный ПК, который позволил бы оценить криптостойкость кодовых последовательностей.

В данной статье приведены примеры ПК, применяемые при оценке криптостойкости кодовых последовательностей с помощью статистических методов оценки, описанные в трудах по системам связи с ШПС, ПСТ NIST и теории нелинейной динамики (табл. 1–3). Отмечено, что в качестве ПК для оценки криптостойкости кодовых последовательностей с помощью статистических методов целесообразно сформировать комплекс ПК. В указанный комплекс следует включить ПК, описанные в табл. 1–3. Сформированный комплекс ПК, по мнению авторов, позволит более точно оценить криптостойкость кодовых последовательностей, используемых в защищенных беспроводных системах связи. Представленные в табл. 1–3 ПК возможно объединить в единый кортеж, который сможет служить обобщенным критерием оценки криптостойкости кодовых последовательностей. Отмечено, что в известных работах [1–8, 10–23], в которых исследуются вопросы оценки криптостойкости кодовых последовательностей, используемых в защищенных беспроводных системах связи, в явном виде такой кортеж не представлен.

Предложена содержательная формулировка задачи повышения защищенности функционирования беспроводной системы связи. Для повышения защищенности функционирования беспроводной системы связи при использовании криптостойких кодовых последовательностей необходимо оперировать обобщенным критерием оценки качества таких последовательностей, основанным на статистических оценках и представляющим собой кортеж, описываемый выражением (1). Дополнительно к этому проведена модернизация кортежа, описываемого с помощью выражения (1), с учетом ПК, отвечающих за надежность. Модифицированный кортеж описывается выражением (2).

По итогам проведенных исследований следует заключить, что при использовании в защищенных беспроводных системах связи криптостойких кодовых последовательностей необходимо обращать внимание на комплекс ПК, описываемый выражением (2). Сформированный обобщенный критерий оценки качества позволит повысить точность оценки криптостойкости кодовых последовательностей при их использовании в защищенных беспроводных системах связи.

СПИСОК ЛИТЕРАТУРЫ

1. Общесистемные вопросы защиты информации / Ред. Е.М. Сухарев. М.: Радиотехника, 2003. 296 с.
2. Панькова В.В., Саломатин С.Б. Криптографический анализ кодовых структур кривой Эрмита на соответствие требованиям систем защиты информации // Доклады БГУИР. 2014. № 3 (81). С. 58–63. URL: <https://libeldoc.bsuir.by/handle/123456789/1280>
3. Гавришнев А.А., Осипов Д.Л. Построение критерия оценки качества двоичных баркероподобных кодов // Т-Comm: Телекоммуникации и транспорт. 2022. Т. 16, № 12. С. 11–16. DOI: 10.36724/2072-8735-2022-16-12-11-16.
4. Navas R.E., Cuppens F., Cuppens N., Toutain L., Papadopoulos G. Physical resilience to insider attacks in IoT networks: Independent cryptographically secure sequences for DSSS anti-jamming // Computer Networks, 2021. Vol. 187. Id. 107751 DOI: 10.1016/j.comnet.2020.107751
5. Горбенко И.Д., Замула А.А. Криптографические сигналы: требования, методы синтеза, свойства, применение в телекоммуникационных системах // Радиотехника (ХНУРЭ). 2016. Вып. 186. С. 7–23. URL: <https://openarchive.nure.ua/items/5da89961-36a4-4b6e-9180-6154ec233eaf>
6. Иванов М.А., Чугунков И.В. Криптографические методы защиты информации в компьютерных системах и сетях. М.: НИЯУ МИФИ, 2012. 400 с.
7. Фомичев В.М., Мельников Д.А. Криптографические методы защиты информации. В 2 ч. Ч. 1. Математические аспекты. М.: Изд-во Юрайт, 2017. 209 с.
8. Гавришнев А.А. Оценка криптостойкости генераторов кодовых последовательностей // Вестник НЦБЖД. 2019. № 4(42). С. 86–91. URL: https://ncbgd.tatarstan.ru/rus/file/pub/pub_2170199.pdf
9. Корячко В.П., Курейчик В.М., Норенков И.П. Теоретические основы САПР. М.: Энергоатомиздат, 1987. 400 с.
10. Варакин Л.Е. Системы связи с шумоподобными сигналами. М.: Радио и связь, 1985. 384 с.
11. Гришенцев А.Ю., Арустамов С.А., Коробейников А.Г., Козин О.В. Защита канала широкополосной связи с применением ортогональных шумоподобных сигнальных символов // Научно-технический вестник информационных технологий, механики и оптики. 2019. Т. 19, № 2. С. 280–291. DOI: 10.17586/2226-1494-2019-19-2-280-291
12. Студеникин А.В., Жук А.П. Моделирование дискретных ортогональных кодовых последовательностей для систем передачи информации // Наукоемкие технологии в космических исследованиях Земли. 2021. Т. 13, № 1. С. 36–43. DOI: 10.36724/2409-5419-2021-13-1-36-43
13. Орел Д.В. Моделирование стохастических систем двоичных квазиортогональных кодовых последовательностей на основе метода функциональных преобразований // Автореф. дис. ... канд. техн. наук. Ставрополь, 2013. 19 с.
14. Гавришнев А.А., Жук А.П. Применение алгоритма Берлекэмпа–Месси для количественного анализа защи-

- щенных систем связи // Прикладная информатика. 2019. Т. 14, № 4 (82). С. 118–134. URL: <https://www.elibrary.ru/item.asp?id=39324218>
15. Wang X., Zhou Sh., Zhang H., Zhang Y. New 4D Discrete Hyperchaotic Map and Its Application in Image Encryption // Research Square. 2022. DOI: 10.21203/rs.3.rs-1564139/v1
 16. Зув М.Ю., Кафаров К.М., Логинов С.С. О взаимосвязи показателей хаотической динамики и статистических характеристик псевдослучайных сигналов на основе нелинейных систем Лоренца и Чуа // Вестник Поволжского государственного технологического университета. Серия: Радиотехнические и инфокоммуникационные системы. 2021. № 2(50). С. 21–29. DOI: 10.25686/2306-2819.2021.2.21
 17. Богаченко Н.Ф., Горохов И.О. Построение генератора псевдослучайных последовательностей на основе клеточного автомата // Математические структуры и моделирование. 2020. № 4(56). С. 64–74. DOI: 10.24147/2222-8772.2020.4.64-74
 18. Альнаджар Х.Х. Оценка качества генератора псевдослучайных чисел на основе нечеткой логики для применения в электронной коммерции // Материалы VII Международной очной научно-практической конференции "Проблемы анализа и моделирования региональных социально-экономических процессов". Казань, 2017. С. 27–30. URL: https://kpfu.ru/staff_files/F459443669/PA2017.pdf
 19. Шахтарин Б.И., Кобылкина П.И., Сидоркина Ю.А., Кондратьев А.В., Митин С.В. Генераторы хаотических колебаний: Учебное пособие. М.: Гелиос АРВ, 2007. 248 с.
 20. Гавришев А.А. Моделирование и количественно-качественный анализ распространенных защищенных систем связи // Прикладная информатика. 2018. Т. 13, № 5. С. 84–122. URL: http://www.appliedinformatics.ru/r/articles/article/index.php?article_id_4=2300
 21. Sun K. Chaotic Secure Communication: Principles and Technologies. Tsinghua University Press and Walter de Gruyter GmbH, 2016. 333 p.
 22. Гавришев А.А., Жук А.П. Применение методов нелинейной динамики для исследования хаотичности сигналов-переносчиков защищенных систем связи на основе динамического хаоса // Вестник НГУ. Серия: Информационные технологии. 2018. Т. 16, № 1. С. 50–60. URL: <https://intechngu.elpub.ru/jour/article/view/19>
 23. Васюта К.С. Классификация процессов в инфокоммуникационных радиотехнических системах с применением BDS-статистики // Проблемы телекоммуникаций. 2012. № 4 (9). С. 63–71. URL: <https://elibrary.ru/item.asp?id=20260336>
 24. Макаренко С.И. Справочник научных терминов и обозначений. СПб.: Научное издание, 2019. 254 с.
 25. Лисничук А.А. Процедура многокритериального синтеза OFDM-радиосигналов для снижения пик-фактора и повышения структурной скрытности систем передачи информации // Вестник Рязанского государственного радиотехнического университета. 2021. № 77. С. 17–28. DOI: 10.21667/1995-4565-2021-77-17-28
 26. Гавришев А.А., Гавришев А.Н. К вопросу о расчете значений пик-фактора сигналов, генерируемых распространенными скрытными системами связи // Вестник НЦБЖД. 2020. № 3(45). С. 149–157. URL: https://ncbgd.tatarstan.ru/rus/file/pub/pub_2478119.pdf

НИЯУ МИФИ, Москва, Россия (Гавришев А.А.)

СКФУ, г. Ставрополь, Россия (Осипов Д.Л.)

Контакты: Гавришев Алексей Андреевич,
alexxx.2008@inbox.ru

Материал поступил в редакцию 18.08.2023

BUILDING OF A GENERALIZED QUALITY ASSESSMENT CRITERION CRYPTOGRAPHIC CODE SEQUENCES USED IN SECURE WIRELESS COMMUNICATION SYSTEMS

A. A. Gavrishev¹, D. L. Osipov²

¹NRNU MEPhI, Moscow, Russia

²NCFU, Stavropol, Russia

The analysis of statistical methods for assessing the cryptographic strength of code sequences used in secure wireless communication systems was carried out. The analysis showed that a universal quality assessment indicator (QAI) for assessing the cryptographic strength of code sequences was not proposed in the well-known works. It is noted that it is advisable to form a QAI complex for assessing the cryptographic resistance of code sequences using statistical methods. The QAIs previously described in the literature are to be included in this set. The formed QAI complex, according to the authors, makes it possible to more accurately assess the cryptographic resistance of code sequences used in secure wireless communication systems. To evaluate the cryptographic resistance of code sequences and to serve as a generalized quality criterion, a single tuple has been developed based on the QAI complex. It is noted that a tuple is not explicitly represented in known papers. The authors have modified the original tuple, taking into account the QAIs, responsible for reliability. The need to pay attention to the QAI complex is revealed in the use of cryptographic code sequences in secure wireless communication systems. The generalized quality assessment criterion will improve the accuracy of assessing the cryptographic resistance of code sequences used in secure wireless communication systems.

Keywords: quality assessment indicators, secure wireless communication systems, code sequences, crypto resistance, statistical methods

REFERENCES

1. Sukharev E.M., ed. *Obshchesistemnye voprosy zashchity informatsii* [System-wide information security issues]. Moscow, Radiotekhnika Publ., 2003. 296 p. (In Russ.).
2. Pankova V.V., Salomatin S.B. [Cryptographic analysis of the code structures of hermite curve for compliance with the requirements of information security systems]. *Doklady BGUIR* [BSUID reports], 2014, no. 3 (81), pp. 58–63. URL: <https://libeldoc.bsuir.by/handle/123456789/1280> (In Russ.).
3. Gavrishev A.A., Osipov D.L. [Building a quality assessment criterion binary barker-like codes]. *T-Comm: Telekommunikatsii i transport* [T-Comm – journal of telecommunications and their application in transport industry], 2022, vol. 16, no. 12, pp. 11–16. DOI: 10.36724/2072-8735-2022-16-12-11-16 (In Russ.).
4. Navas R.E., Cuppens F., Cuppens N., Toutain L., Papadopoulos G. Physical resilience to insider attacks in IoT networks: Independent cryptographically secure sequences for DSSS anti-jamming. *Computer Networks*, 2021, vol. 187, id. 107751. DOI: 10.1016/j.comnet.2020.107751
5. Gorbenko I.D., Zamula A.A. [Cryptographic signals: requirements, synthesis methods, properties, application in telecommunication systems]. *Radiotekhnika (KhNUREh)* [Radio engineering (KhNURE)], 2016, no. 186, pp. 7–23. URL: <https://openarchive.nure.ua/items/5da89961-36a4-4b6e-9180-6154ec233eaf> (In Russ.).
6. Ivanov M.A., Chugunkov I.V. *Kriptograficheskie metody zashchity informatsii v komp'yuternykh sistemakh i setyakh* [Cryptographic methods of information protection in computer systems and networks]. Moscow: NIYaU MIFI Publ., 2012. 400 p. (In Russ.).
7. Fomichev V.M., Mel'nikov D.A. *Kriptograficheskie metody zashchity informatsii. V 2 ch. Ch. 1. Matematicheskie aspekty* [Cryptographic methods of information protection. At 2 parts. Part 1. Mathematical aspects]. Moscow: Yurait Publ., 2017. 209 p. (In Russ.).
8. Gavrishev A.A. [Assessment of the crypto resistance of the generators of code sequences]. *Vestnik NTsBZhD* [Bulletin of the NCBhD], 2019, no. 4(42), pp. 86–91. (In Russ.). URL: https://ncbgd.tatarstan.ru/rus/file/pub/pub_2170199.pdf
9. Koryachko V.P., Kureichik V.M., Norenkov I.P. *Teoreticheskie osnovy SAPR* [Theoretical foundations of CAD]. Moscow, Energoatomizdat Publ., 1987. 400 p. (In Russ.).
10. Varakin L.E. *Sistemy svyazi s shumopodobnymi signalami* [Noise-like communication systems]. Moscow, Radio i svyaz' Publ., 1985. 384 p. (In Russ.).
11. Grishentsev A.Yu., Arustamov S.A., Korobeynikov A.G., Kozin O.V. [Orthogonal noise-like signal symbols for broadband channel protection]. *Nauchno-tehnicheskii vestnik informatsionnykh tekhnologii, mekhaniki i optiki* [Scientific and Technical Journal of Information Technologies, Mechanics and Optics], 2019, vol. 19, no. 2, pp. 280–291. DOI: 10.17586/2226-1494-2019-19-2-280-291 (In Russ.).

12. Studenikin A.V., Zhuk A.P. [Modeling of discrete orthogonal code sequences for information transmission systems]. *Naukoemkie tekhnologii v kosmicheskikh issledovaniyakh Zemli* [High technologies in Earth space research], 2021, vol. 13, no. 1, pp. 36–43. DOI: 10.36724/2409-5419-2021-13-1-36-43 (In Russ.).
13. Orel D.V. *Modelirovanie stokhasticheskikh sistem dvoichnykh kvaziortogonal'nykh kodovykh posledovatel'nostei na osnove metoda funktsional'nykh preobrazovaniy*. Avtoref. diss. kand. techn. nauk. [Simulation of stochastic systems of binary quasi-orthogonal code sequences based on the method of functional transformations. Abstract cand. techn. sci. diss.]. Stavropol, 2013. 19 p. (In Russ.).
14. Gavrishev A.A., Zhuk A.P. [The application of the algorithm Berlekamp-Massey for the quantitative analysis of secure communication systems]. *Prikladnaya informatika* [Journal of applied informatics], 2019, vol. 14, no. 4 (82), pp. 118–134. (In Russ.).
URL: <https://www.elibrary.ru/item.asp?id=39324218>
15. Wang X., Zhou Sh., Zhang H., Zhang Y. New 4D Discrete Hyperchaotic Map and Its Application in Image Encryption. *Research Square*, 2022. DOI: 10.21203/rs.3.rs-1564139/v1
16. Zuev M.Y., Kafarov K.M., Loginov S.S. [On the relation between indicators of chaotic dynamics and statistical characteristics of pseudo-random signals based on nonlinear systems of Lorentz and Chua]. *Vestnik Povolzhskogo gosudarstvennogo tekhnologicheskogo universiteta. Seriya: Radiotekhnicheskie i infokommunikatsionnye sistemy* [Vestnik of Volga State University of Technology. Series "Radio engineering and infocommunication systems"], 2021, no. 2(50), pp. 21–29. DOI: 10.25686/2306-2819.2021.2.21 (In Russ.).
17. Bogachenko N.F., Gorohov I.O. [Construction of a pseudo-random sequence generator based on a cellular automaton]. *Matematicheskie struktury i modelirovanie* [Mathematical structures and modeling], 2020, no. 4(56), pp. 64–74. DOI: 10.24147/2222-8772.2020.4.64-74 (In Russ.).
18. Al'nadzhazh Kh.Kh. [Evaluation of pseudo-random number generator quality based on fuzzy logic for e-commerce applications]. *Materialy VII Mezhdunarodnoi ochnoi nauchno-prakticheskoi konferentsii "Problemy analiza i modelirovaniya regional'nykh sotsial'no-ehkonomicheskikh protsessov"* [Proc. VII Int. full-time sci. pract. conf. "Problems of analysis and modeling of regional socio-economic processes"]. Kazan, 2017. pp. 27–30.
URL: https://kpfu.ru/staff_files/F459443669/PA2017.pdf (In Russ.).
19. Shakhrtarin B.I., Kobylkina P.I., Sidorkina Yu.A., Kondrat'ev A.V., Mitin S.V. *Generatory khaoticheskikh kolebaniy: Uchebnoe posobie* [Chaotic oscillation generators: Tutorial]. Moscow, Gelios ARV Publ., 2007. 248 p. (In Russ.).
20. Gavrishev A.A. [Modeling and quantitative and qualitative analysis of common secure communication systems]. *Prikladnaya informatika* [Journal of applied informatics], 2018, vol. 13, no. 5, pp. 84–122. (In Russ.). URL: http://www.appliedinformatics.ru/r/articles/article/index.php?article_id_4=2300
21. Sun K. *Chaotic Secure Communication: Principles and Technologies*. Tsinghua University Press and Walter de Gruyter GmbH, 2016. 333 p.
22. Gavrishev A.A., Zhuk A.P. [Application of methods of nonlinear dynamics to study the chaotic state of the carrier signals of secure communication systems based on dynamic chaos]. *Vestnik NGU. Seriya: Informatsionnye tekhnologii* [Vestnik NSU. Series: Information Technologies], 2018, vol. 16, no. 1, pp. 50–60. (In Russ.). URL: <https://intechngu.elpub.ru/jour/article/view/19>
23. Vasyuta K.S. [Classification of processes in information and communication radio engineering systems using BDS statistics]. *Problemy telekommunikatsii* [Telecommunications issues], 2012, no. 4 (9), pp. 63–71.
URL: <https://elibrary.ru/item.asp?id=20260336>
24. Makarenko S.I. *Spravochnik nauchnykh terminov i oboznachenii* [Handbook of scientific terms and designations]. Saint Petersburg, Naukoemkie tekhnologii Publ., 2019. 254 p. (In Russ.).
25. Lisnichuk A.A. [Multi-criteria synthesis procedure of ofdm-signals to increase energy efficiency and structural hiding of communication radio systems]. *Vestnik Ryazanskogo gosudarstvennogo radiotekhnicheskogo universiteta* [Vestnik of Ryazan State Radio Engineering University], 2021, no. 77, pp. 17–28. DOI: 10.21667/1995-4565-2021-77-17-28 (In Russ.).
26. Gavrishev A.A., Gavrishev A.N. [To the question of calculating the crest factor values of signals generated by common hidden communication systems]. *Vestnik NTsBZhD* [Bulletin of the NCBhD], 2020, no. 3(45), pp. 149–157. (In Russ.). URL: https://ncbgd.tatarstan.ru/rus/file/pub/pub_2478119.pdf

Contacts: *GavrishevAleksiejAndreevich*,
alexxx.2008@inbox.ru

Article received by the editorial office on 18.08.2023

INTRODUCTION

Modern secure wireless communication systems must function reliably under conditions of destabilizing external influences, for example, when a third party intercepts transmitted signals or during radio-electronic signal suppression. This determines the constant improvement of methods for increasing the security of wireless communication systems, which makes it possible to increase the level of a priori uncertainty in the parameters and characteristics of transmitted signals [1–8]. Among the countermeasures approaches, cryptographic methods of information protection and technologies based on the transmission of noise-like signals (NLS) stand out. When using cryptographic methods for protecting information or signal transmission technologies based on NPS, it is important to correctly select high-quality code sequences with the help of which the transmitted information is converted into a form that cannot be read by an unauthorized user. Thus, the task of assessing the quality of code sequences used in secure wireless communication systems is certainly relevant.

Currently, the analysis of code sequences used in secure wireless communication systems can be carried out using various techniques. Most researchers believe that one of the primary indicators is the cryptographic strength of code sequences used in secure wireless communication systems [1–8]. Typically, the cryptographic strength of code sequences is understood as their resistance to security violations, which is characterized by a number of quality assessment indicators (QAIs), among which the following are often highlighted [1–8]:

1. Based on the known final part of the code sequence, it is impossible to determine both its subsequent element and its previous one.
2. Indistinguishability of the statistical properties of the generated code sequences from similar properties of a true random sequence.
3. Long sequence period.
4. A slight change in the initial conditions should lead to a significant unpredictable change in the output code sequence.

Despite the fact that assessing the cryptographic strength of code sequences is still a difficult task, such an assessment makes it possible to identify possible defects in the method of generating a sequence and assess its acceptability in terms of the resistance of the sequence to disclosure by an attacker. Therefore, further research in this area is an important area of ensuring the protection of information transmitted using wireless communication systems and requires further study [1–8].

The purpose of this article is to improve the accuracy of assessing the cryptographic strength of code sequences used in secure wireless communication sys-

tems through the use of the identified generalized criterion.

The objective of this article is to construct a general criterion for assessing the quality of crypto-strong code sequences used in secure wireless communication systems based on statistical estimates of cryptographic strength.

MAIN PART

According to [1–9], existing methods for assessing the cryptographic strength of code sequences used in secure wireless communication systems can be divided into two large groups: analytical methods and statistical methods.

Analytical methods make it possible to obtain the characteristics of a system as a certain function of its operating parameters. Typically, an analytical model represents a set of mathematical expressions and relationships, the solution to which yields the parameters necessary to evaluate the system under study. Often, these parameters are probabilistic or other characteristics.

Statistical methods are based on computer modeling of the behavior of real objects, processes, and systems over a given period of time and repeated reproduction of behavior for statistical processing of the obtained data in order to verify their adequacy. For the sake of simplification, we will focus in more detail on statistical methods for assessing the cryptographic strength of code sequences. Currently, researchers have proposed a wide range of statistical methods for assessing cryptographic strength, but among them, there is no universal QAI for assessing the cryptographic strength of code sequences.

Tab. 1 shows widely used PCs used in NLS communication systems [1–5, 7, 8, 10–14]. Using QAI data, the cryptographic strength of code sequences used in wireless communication systems is assessed.

Tab. 1. Examples of QAIs for assessing the cryptographic strength of code sequences using statistical methods described in works on NLS communication systems

More recent publications [7, 15–18] show that one of the most popular statistical tools for assessing the cryptographic strength of code sequences used in secure wireless communication systems is testing such as the D. Knuth test, diehard, NIST, etc. Of the tests mentioned, the most popular in practice is the NIST package of statistical tests (PST NIST).

In order to reduce time and computational costs, the tests included in PST NIST and noted in Tab. 2 are

usually preferred for assessing the cryptographic strength of code sequences [7, 15–18].

Tab. 2. Examples of QAIs for assessing the cryptographic strength of code sequences using statistical evaluation methods presented in the NIST statistical test package

Each statistical test presented in Tab. 2 solves the problem of testing the hypothesis about the cryptographic strength of the input code sequence (null hypothesis) or an alternative hypothesis (the code sequence is not resistant).

Another tool for assessing the cryptographic strength of code sequences used in secure wireless communication systems is the theory of nonlinear dynamics [15, 16, 19–23]. Tab. 3 lists some of these QAIs.

Tab. 3. Examples of QAIs for assessing the cryptographic strength of code sequences using statistical methods based on the theory of nonlinear dynamics

At the moment, QAIs presented in Tab. 3 have not been widely used for assessing the cryptographic strength of code sequences. However, their use for

these purposes is promising because they make it possible to distinguish the structure of code sequences and carry out their classification.

The analysis of the literature [1–8, 10–23] shows that it is advisable to form a QAI complex for assessing the cryptographic strength of code sequences using statistical methods. It is advisable to include the QAIs described in Tabs. 1–3 into this complex. The formed QAI complex, according to the authors, will make it possible to more accurately assess the cryptographic strength of code sequences used in secure wireless communication systems. QAIs described in Tabs. 1–3 can be combined into a single tuple, which serves as a general criterion for assessing the cryptographic strength of code sequences. Note that in the known works [1–8, 10–23], which study the issues of assessing the cryptographic strength of code sequences used in secure wireless communication systems, such a tuple is not presented explicitly.

By analogy with [3] and according to methodological recommendations from [24], we write out a meaningful formulation of the problem of increasing the security of the functioning of a wireless communication system. To increase the security of a wireless communication system operating when using cryptoresistant code sequences, it is necessary to set a general criterion for assessing the quality of such sequences. The criterion is based on statistical estimates and represents a tuple (1):

$$\langle R_{A \max}(\tau), R_{C \max}(\tau), Q, N, L, T_1, T_2, T_3, T_4, T_5, \lambda_{\max}, H, \omega(\varepsilon) \rangle, \quad (1)$$

in which:

$$\begin{cases} R_{A \max}(\tau) < R_{A \max \text{ don}}(\tau), R_{C \max}(\tau) < R_{C \max \text{ don}}(\tau), Q \rightarrow \max, \\ N \rightarrow \max, L > \frac{N}{2}, T_1 \rightarrow 0.5, T_2 \rightarrow 0.5, T_3 \rightarrow 0.5, T_4 \rightarrow 0.5, \\ T_5 \rightarrow 0.5, \lambda_{\max} \rightarrow \max, H \rightarrow 0.5, \omega(\varepsilon) < \omega_{\text{don}}(\varepsilon). \end{cases}$$

Here $R_{A \max}(\tau)$, $R_{C \max}(\tau)$, Q , N , L are QAIs presented in Tab. 1; T_1 , T_2 , T_3 , T_4 , T_5 are QAIs according to Tab. 2; $\lambda_{\max}$, H , $\omega(\varepsilon)$ are QAIs according to Tab. 3; $R_{A \max \text{ don}}(\tau)$ is the permissible value of the side peaks of the autocorrelation function, $R_{C \max \text{ don}}(\tau)$ is the permissible value of the side peaks of the cross-correlation, $\omega_{\text{don}}(\varepsilon)$ is the permissible value of the BDS statistics of code sequences.

In addition to this, we modernize the presented tuple, taking into account the QAIs responsible for reliability [3, 10, 12, 25, 26], in particular the crest factor of code sequences ρ and outliers of their amplitude-frequency spectra $G(\omega)$, to the following final form (2):

$$\langle R_{A \max}(\tau), R_{C \max}(\tau), Q, N, L, T_1, T_2, T_3, T_4, T_5, \lambda_{\max}, H, \omega(\varepsilon), \rho, G(\omega) \rangle, \quad (2)$$

where

$$\begin{cases} R_{A \max}(\tau) < R_{A \max \text{ } \text{don}}(\tau), R_{C \max}(\tau) < R_{C \max \text{ } \text{don}}(\tau), Q \rightarrow \max, \\ N \rightarrow \max, L > \frac{N}{2}, T_1 \rightarrow 0.5, T_2 \rightarrow 0.5, T_3 \rightarrow 0.5, T_4 \rightarrow 0.5, \\ T_5 \rightarrow 0.5, \lambda_{\max} \rightarrow \max, H \rightarrow 0.5, \omega(\varepsilon) < \omega_{\text{don}}(\varepsilon), \rho < \rho_{\text{don}}, G(\omega) < G_{\text{don}}(\omega). \end{cases}$$

Here, in addition to the indicators according to (1), ρ is the crest factor of the code sequences, $G(\omega)$ are the outliers of the amplitude-frequency spectra of the code sequences, ρ_{don} is permissible crest factor of code sequences, $G_{\text{don}}(\omega)$ are permissible outliers of amplitude-frequency spectra of code sequences.

CONCLUSION

Currently, statistical methods for assessing the cryptographic strength of code sequences used in secure wireless communication systems are widely presented in the scientific literature [1–8, 10–23]. However, the authors of these publications have not proposed a universal QAI that would allow assessing the cryptographic strength of code sequences.

This article provides examples of QAIs used in assessing the cryptographic strength of code sequences using statistical assessment methods described in works on NLS communication systems, PST NIST and the theory of nonlinear dynamics (Tabs. 1–3). It is advisable to form a QAI complex instead of using a single QAI for assessing the cryptographic strength of code sequences by means of statistical methods. The specified complex should include the QAIs described in Tabs. 1–3. The formed QAI complex, according to the authors, will make it possible to more accurately assess the cryptographic strength of code sequences used in secure wireless communication systems. QAIs

presented in Tabs. 1–3 can be combined into a single tuple, which can serve as a general criterion for assessing the cryptographic strength of code sequences. It is noted that in well-known works [1–8, 10–23], in which the issues of assessing the cryptographic strength of code sequences used in secure wireless communication systems have been studied, such a tuple is not presented explicitly.

A meaningful formulation of the problem of increasing the security of the functioning of a wireless communication system is proposed. To increase the operating security of a wireless communication system using cryptographically strong code sequences, it is necessary to set a general criterion for assessing the quality of such sequences; the criterion should be based on statistical estimates and represent a tuple described by expression (1). In addition to this, the tuple described using expression (1) was modernized, taking into account the QAIs responsible for reliability. The modified tuple is described by expression (2).

Based on the results of the research, it should be concluded that when using crypto-resistant code sequences in secure wireless communication systems, it is necessary to pay attention to the QAI complex described by expression (2). The generated generalized quality assessment criterion will improve the accuracy of assessing the cryptographic strength of code sequences when used in secure wireless communication systems.