DOI 10.66032/2221-2574-2025-1-1-68-76 УДК 681.535: 656.6

ПРИМЕНЕНИЕ КОДОВ ХЭММИНГА В КАНАЛЕ СВЯЗИ С ДИНАМИЧЕСКОЙ СМЕНОЙ КЛЮЧЕЙ ДЛЯ БЕЗЭКИПАЖНОГО СУДОВОЖДЕНИЯ

Ямпурин Николай Петрович
доктор технических наук, профессор, профессор кафедры «Конструирование и технология РЭС» Арзамасского политехнического института[1] (филиала) ФГБОУ ВО «Нижегородский государственный технический университет им. Р.Е. Алексеева».
E-mail: kitres@apingtu.edu.ru

Крит Андрей Александрович
заведующий лабораторией ФГБОУ ВО «Волжский государственный университет водного транспорта»[2].

Кораблёв Егор Денисович
заведующий лабораторией ФГБОУ ВО «Волжский государственный университет водного транспорта»[2].

Логинов Вячеслав Иванович
кандидат технических наук, доцент ФГБОУ ВО «Волжский государственный университет водного транспорта»[2].

Степанова Алла Сергеевна
кандидат филологических наук, доцент ФГБОУ ВО «Волжский государственный университет водного транспорта»[2].

Федосенко Юрий Семёнович
доктор технических наук, профессор, заведующий кафедрой ФГБОУ ВО «Волжский государственный университет водного транспорта»[2].

[1]*Адрес:* 607220, Российская Федерация, Нижегородская обл., г. Арзамас, ул. К. Маркса, д. 36.
[2]*Адрес:* 603950, Российская Федерация, Нижний Новгород, ул. Нестерова, д. 5.

Аннотация: Рассмотрена возможность использования контроля над целостностью блочной битовой последовательности с помощью алгоритма Хэмминга для последовательности, формируемой в результате работы модифицированного алгоритма Эль-Гамаля и передаваемой через каналы связи, подверженные помехам. Анализируется обработка данных в системе для повышения криптостойкости, а также предлагается метод для повышения помехозащищённости.

Ключевые слова: автоматизация, гаммирование, беспроводная связь, управление безэкипажным судном, линейный генератор псевдослучайной последовательности, избыточное кодирование, алгоритм Хэмминга, модифицированный алгоритм Эль-Гамаля.

Введение

Современная задача защиты информации и сохранения целостности данных, передаваемых по беспроводным каналам связи для управления подвижными объектами и обмена данными, актуализирует необходимость применения эффективных методов кодирования информации. Данный вопрос следует рассматривать в двух аспектах.

Во-первых, через призму резолюции MSC.428(98) — Управление морскими киберрисками в системах управления безопасностью Комитета по безопасности на море Международной морской организации (ИМО) [1], которая призывает обеспечить учёт киберрисков при управлении безэкипажными судами.

Во-вторых, через опыт внедрения беспилотных судов для научно-исследовательской деятельности [2], где многие действия могут проводится, как на воде, так и под водой, поэтому основной акцент делается на автоматизированные комплексы и беспилотные систе-

мы, в частности, безэкипажные катера и беспилотные подводные аппараты. И здесь самое главное звено — это системы управления и связи.

И в первом, и во втором случаях системам управления и связи безэкипажных судов и катеров (далее просто безэкипажных судов) приходится преодолевать зону радиоэлектронного воздействия, что требует соответствующих технических решений.

Определение понятия безэкипажное судно (БЭС) дано в ГОСТ Р 59298-2021: это судно, управляемое внешним оператором, или автономной бортовой системой управления [3]. При управлении судном внешним оператором (с берегового центра управления безэкипажными судами) встаёт задача обеспечения защиты передаваемой информации и сохранения целостности данных. Среди методов, позволяющих решить первую задачу, особое место занимают методы гаммирования, базирующиеся на сверхточных алгоритмах, в частности, на генераторах псевдослучайных последовательностей (ПСП) [4-6].

Важным аспектом применения генераторов ПСП является их способность обеспечивать заданную криптостойкость и быстродействие, особенно при использовании на подвижных объектах, к коим относится БЭС. Одним из основных методов повышения криптостойкости при шифровании информации с использованием генераторов ПСП с равномерным распределением является динамическая смена ключей шифрования. Это достигается путём внедрения в исходный алгоритм шифрования механизма замены ключа шифрования для каждого блока. Такой подход приводит к значительному увеличению криптостойкости получаемого шифра благодаря периодической смене ключей шифрования [7].

В качестве метода, позволяющего вести контроль над целостностью доставляемого сообщения, авторы предлагают использовать алгоритм расчёта битов паритета, основанный на кодах Хэмминга [8]. Выбор в пользу этого алгоритма обусловлен его способностью к самовосстановлению принятой битовой последовательности и удобством применения при блочной передаче данных [9].

Однако использование кодов Хэмминга связано с введением дополнительных (проверочных) символов [8], а это приводит к увеличению объёма передаваемых данных, поэтому необходима их оценка, что позволит оптимизировать процесс передачи данных, учитывая текущие условия работы системы управления и связи.

Цель данной работы – на основе модифицированного алгоритма Эль-Гамаля [7] разработать алгоритм оценки увеличения объёма данных при использовании кодов Хэмминга, в зависимости от размера передаваемого блока и числа проверочных символов, исследовать возможности восстановления принятого сообщения

Постановка задачи

Для достижения сформулированной цели необходимо решить следующие задачи:

1. Внедрить коды Хэмминга в модифицированный алгоритм Эль-Гамаля для повышения помехозащищённости.
2. Разработать алгоритм автоматической оценки увеличения объёма данных при использовании кодов Хэмминга.
3. Провести анализ эффективности использования кодов Хэмминга с точки зрения снижения вероятности появления ошибок.

Анализ криптостойкости модификации алгоритма Эль-Гамаля

Авторами предложен модифицированный алгоритм Эль-Гамаля [13], который предназначен для повышения криптографической стойкости за счёт увеличения длины ключа передаваемого сообщения.

Кроме того, для повышения помехозащищённости передаваемой информации планируется использование кодов Хэмминга в совокупности с вышеописанным алгоритмом. Эти коды позволяют обнаруживать и исправлять ошибки, возникающие в процессе передачи

данных, что существенно увеличивает надёжность системы в условиях помех.

Покажем, что интеграция модифицированного алгоритма Эль-Гамаля и кодов Хэмминга создаёт более устойчивую и защищённую систему обработки и передачи информации. Для этого рассмотрим более подробно работу модифицированного алгоритма Эль-Гамаля [7], в котором существует несколько ключевых параметров, используемых в данной работе:

p — достаточно большое простое число, модуль;

M — байт исходного символа;

g — генеративный ключ (первообразные корни p);

x — секретный ключ;

k — случайное число, взаимно простое с $p - 1$;

a — первая часть зашифрованного сообщения;

b — вторая часть зашифрованного сообщения.

Далее рассмотрим предложенный в [7] алгоритм работы. Сначала генерируется p, а потом для него рассчитываются все первообразные корни g. Затем, для каждого нового M с определённым линейным либо нелинейным шагом выбирается g из заранее рассчитанного набора первообразных корней. И вновь выбранный g применяется в качестве полинома в генераторе (ПСП) на основе регистра сдвига с линейной обратной связью (РСЛОС) [9], что на каждой итерации даёт новую ПСП. Затем, по определённому алгоритму и с учётом условий $1 < x,\ k < p - 1$ из новой ПСП выбирается два числа, которые становятся новыми x и k. Применение такого метода позволит избежать одинаковых g, x и k, для случая, когда в качестве ключа используется M, так как M_{i-1} может быть равно M_i. В таблице 1 приведён пример работы разработанного алгоритма для сообщения «Грамм».

Можно заметить, что хотя на шагах 3 и 4 значения M одинаковы, но шифротексты отличны друг от друга за счёт применения разных g.

В данном методе необходимо учитывать, что количество первообразных корней конечно, что накладывает ограничения на длину исходного текста. Для увеличения размерности текста нужно использовать достаточно большие p. Так, например, для применённого в таблице 1 параметра $p = 1009$ существует 288 первообразных корней, а для ближайшего к нему $p = 1013$ их число возрастает уже до 440. Поскольку данная зависимость не является линейной, то существуют некоторые последующие p, для которых количество первообразных корней значительно меньше, чем для предыдущего p. Например, для $p = 1019$ существует 508 корней, а для $p = 1021$ их всего 256.

Оценим приблизительную криптостойкость рассматриваемого модифицированного алгоритма. Так как основным ключом является открытый ключ p, оценка будет происходить для его разрядности 8. Решение взлома будет основано на переборе генерируемых g, x и k. Пара ключей $(x,\ k)$ определяется не только ключом g, но также и p. Дадим оценку минимального количества $g(p)$ и $(x,\ k)\ (g(p),\ p)$. Согласно последовательности A008330 [11] минимальным значением отношения p к g будет значение 2. Данное значение было подтверждено моделированием разрядности от 1 до 13. Всего получено 1228 значений p, результаты расчёта приведены на рис. 1, *а*), где в виде линии при-

Таблица 1. Работа модифицированного алгоритма

№	p	Исходный текст	M	a	b	g	x	k
0	1009	Г	195	308	651	97	204	71
1		р	240	994	589	318	492	932
2		а	224	289	865	17	21	2
3		м	236	179	875	83	225	189
4		м	236	781	871	281	562	937

ведён рост значения p, а разброс количества первообразных корней g представлен в виде точек, в зависимости от текущего p. А на рис. 1, *б*) приведён график отношения текущего p к $g(p)$, позволяющий оценить минимально возможное количество первообразных ключей для текущего p.

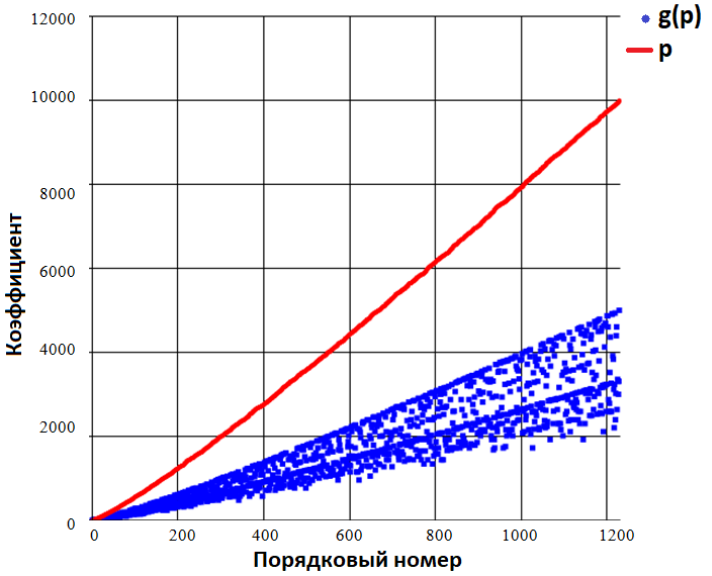
Тогда минимальная оценка количества $g(p) = p/2$. Для каждой пары $(g(p), p)$ существует своя пара (x, k), когда всего существует $x = p^{2/4}$ и $k = p^{2/4}$. Тем самым, общая комбинация пары $(x, k) = (p^{2/4})^2 = p^{4/16}$. Для известного количества $g(p)$ получаем общее количество комбинаций на одно p, равное $p^{5/32}$. Отсюда получаем приблизительную оценку для длины ключа:

– $N_4 = ((2^4)^5)/32 = 2^{15}$ — длина ключа 15 бит,

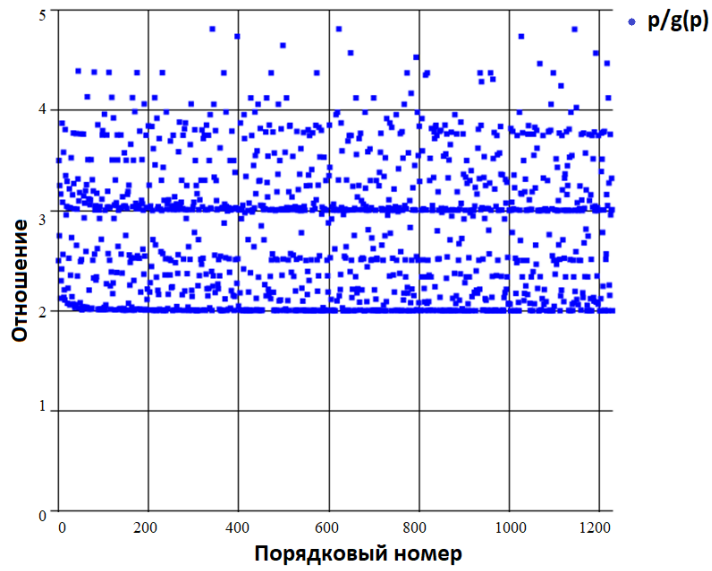
– $N_8 = ((2^8)^5)/32 = 2^{35}$ — длина ключа 35 бит,

– $N_{16} = ((2^{16})^5)/32 = 2^{75}$ — длина ключа 75 бит,

– $N_{32} = ((2^{32})^5)/32 = 2^{155}$ — длина ключа 155 бит.



а) разброс первообразных корней g(p)



б) график отношения p/g(p)

Рис. 1.

Расчёт параметров сообщения с кодами Хэмминга

Как было сказано выше, применим для контроля целостности передаваемого сообщения (битовой посылки) кодирование по Хэммингу. Работа данного алгоритма заключается в следующем: исходное сообщение разбивается на блоки определённой длины, и затем, в зависимости от размера блока, рассчитывается строго определённое число битов паритета, используемых в приёмном устройстве для контроля целостности сообщения, и в случае, если принятое сообщение является изменённым относительно переданного, то данное сообщение восстанавливается по алгоритму Хэмминга. Применение данной избыточности используется в модифицированном алгоритме Эль-Гамаля для надёжного контроля передачи открытых ключей ***(a, b)***, так как от них зависит корректность принятого и декодированного сообщения.

Для решения поставленной задачи эмпирическим путём была выведена и в дальнейшем использована система уравнений, по которой рассчитывается длина одного блока с битами паритета:

$$\begin{cases} x = \log_2 n, \\ y = n + x + 1, \end{cases} \quad (1)$$

где y — размер кодированного блока; x — количество разрядов, используемых для описания одного блока сообщения; n — размер исходного блока.

Приведём пример решения системы уравнений (1).

Пусть M = 64 бита — длина исходного сообщения, а n = 8 бит — размер исходного блока; тогда $x = \log_2(n) = \log_2(8) = 3$, а $y = 2^x + x + 1 = 2^3 + 3 + 1 = 12$ бит — размер кодированного блока с учётом добавленных битов паритета.

Теперь рассчитаем длину полного сообщения с учётом полученных параметров:

$K = M/n = 64/8 = 8$ — количество пакетов на основе размера исходного блока;

$M \cdot n = K \cdot y = 8 \cdot 12 = 96$ бит — полная длина нового сообщения.

На основе системы (1) был написан алгоритм, позволяющий вычислить зависимость длины сообщения с избыточными битами к длине сообщения без битов паритета. На рис. 2 построена соответствующая зависимость: по оси абсцисс расположена степень, означающая x, а по оси ординат — коэффициент зависимости, описанный выше.

В таблице 2 приведены значения коэффициентов в зависимости от размерности блока.

Видно, что коэффициент зависимости с ростом разрядности x стремится к 1, а длина блока с битами паритета нелинейно увеличивается. Благодаря вычисленным коэффициентам, можно делать вывод о том, какой объем памяти займёт в буфере передаваемое сообщение и оценить его избыточность.

Определение минимального кодового расстояния для безошибочной передачи сообщения

Минимальное кодовое расстояние (расстояние Хэмминга) – это число позиций, в которых два кодовых слова различаются, и именно оно служит основным показателем для оценки эффективности кодирования [8]. Коды Хэмминга с минимальным расстоянием 3 способны не только обнаруживать, но и исправлять одну ошибку в кодовом слове. Это достигается бла-

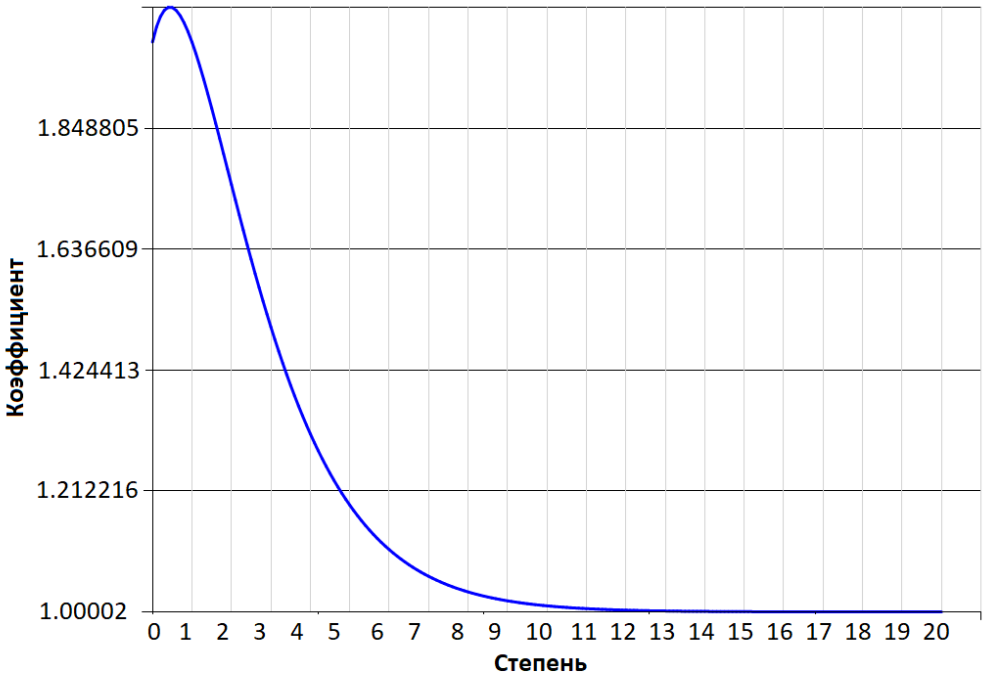


Рис. 2. График зависимости размера блоков от степени

Таблица 2. Коэффициенты зависимости

Разрядность, x	Коэффициент зависимости, y/n	Размер кодированного блока, y	Размер исходного блока, n
0	2	2	1
1	2	4	2
2	1,75	7	4
3	1,5	12	8
4	1,3125	21	16
5	1,1875	38	32
6	1,109375	71	64
7	1,0625	136	128
8	1,03515625	265	256
9	1,01953125	522	512
10	1,0107421875	1035	1024
11	1,005859375	2060	2048
12	1,003173828125	4109	4096
13	1,001708984375	8206	8192
14	1,00091552734375	16399	16384
15	1,00048828125	32784	32768
16	1,00025939941406	65553	65536
17	1,00013732910156	131090	131072
18	1,00007247924805	262163	262144
19	1,00003814697266	524308	524288
20	1,00002002716064	1048597	1048576

годаря тому, что, если произошло искажение одного бита, система может определить, какое из возможных кодовых слов было отправлено, и восстановить информацию.

Однако, для достижения максимальной эффективности важно учитывать условия передачи данных, а именно — вероятность возникновения ошибок на канале связи. При повышении вероятности ошибок необходимость в использовании кодов с большим минимальным расстоянием становится очевидной. Например, если минимальное расстояние Хэмминга равно 2, код сможет только обнаруживать ошибки, но не исправлять их, что может быть недостаточно в условиях нестабильного канала связи.

В рамках анализа эффективности кодов Хэмминга необходимо провести расчёт вероятности появления ошибок. Применение такой модели канала, как бинарная симметричная модель, позволяет оценить влияние частоты появления ошибок на общую надёжность передачи данных. Коды Хэмминга могут быть адаптированы к конкретным условиям передачи, обеспечивая оптимальное соотношение между избыточностью данных и уровнем надёжности [16].

Итак, после дополнения канала связи алгоритмом Хэмминга, рассмотрим, какое минимальное расстояние получается в результате подачи на выход передатчика битовой последовательности (с учётом битов паритета). Возьмём для примера то же сообщение, что было применено в таблице 1: слово «Грамм». В результате шифрования и перевода в битовую последовательность было получено следующее кодовое слово: «00000001011011111 10000000100010001110000000100101110110000 00001100000001100000001100101000100000000 01010111101000000000000000011000000000011 10110010000000001101101010000000100101010 00100000000000000001000000000000000010 00000000000000001000000000000000010000». Обработка данного сообщения позволила разбить его на блоки по 8 бит, что, согласно таблице 2, для $x = 3$ даёт размер кодированного блока в 12 бит при кодировании по Хэммингу. В таблице 3 приведены полученные кодовые слова.

Таблица 3. Кодовые слова

1: 000100010001
2: 110111001111
3: 011110000000
4: 110110010100
5: 000111100000
6: 000100110010
7: 111011001100
8: 100000000110
9: 110100000011
10: 000100010001
……
27: 000100010001
28: 000000000000
29: 000000000000
30: 100110000000
31: 000000000000
32: 110100100000

После дальнейшей обработки данных кодовых слов было выявлено, что минимальное расстояние Хэмминга равно 3, что позволяет обнаружить до двух ошибок и исправить одну ошибку. На рис. 3 приведены результаты передачи и приёма закодированного сообщения «Грамм».

Как видно из рис. 3, разрабатываемая система действительно обнаружила одну ошибку, исправила её и смогла восстановить отправленное сообщение.

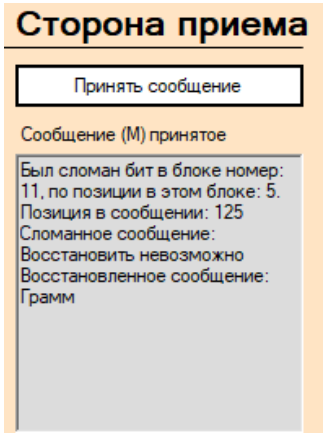


Рис. 3. Принятое и восстановленное сообщения

Выводы

1. Предложен комплексный подход к использованию модифицированного алгоритма Эль-Гамаля с динамической сменой параметров (ключей) совместно с кодированием по Хеммингу сообщений, позволяющих увеличить защищённость системы управления безэкипажным судном внешним оператором от воздействия различных внешних факторов.

2. Разработан алгоритм оценки увеличения объёма данных в зависимости от размера передаваемого блока и объёма избыточного кодирования. Предложен алгоритм расчёта кодового расстояния и проанализировано его влияние на разработанную систему защиты информации.

Литература

1. Resolution MSC.428(98) [Электронный ресурс]: International Maritime Organization. URL: https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf (дата обращения: 25.11.2024).

2. В Севастополь из Петербурга отправилось первое российское научно-исследовательское судно беспилотник [Электронный ресурс] // Российская газета. 2022. URL: https://rg.ru/2022/08/30/reg-ufo/v-sevastopol-iz-peterburga-otpravilos-pervoe-rossijskoe-nauchno-issledovatelskoe-sudno-bespilotnik.html?ysclid=m7p53a9q4e446713553 (дата обращения: 25.11.2024).

3. ГОСТ Р 21.1101 2020. Основные требования к проектной и рабочей документации. М.: Стандартинформ, 2021. 12 с.

4. *Смарт Н.* Криптография: учебник; пер. с англ. М.: Техносфера, 2006. 525 с.

5. *Слеповичев И.И.* Генераторы псевдослучайных чисел. Саратов: СГУ, 2017. 118 с.

6. *Фергюссон Н. Шнайер Б.* Практическая криптография. М.: Вильямс, 2005. 424 с.

7. *Iampurin N.P. Krit A.A. Korablev E.D. Loginov V.I. Fedosenko I.S.* Implementation of an Encoding System with Dynamic Key Change Based on Pseudorandom Sequence Generators // 2024 Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO). Vyborg, Russian Federation, 2024. Pp. 1–5. DOI: 10.1109/SYNCHROINFO61835.2024.10617466.

8. *Питерсон У. Уэлдон Э.* Коды, исправляющие ошибки / под ред. *Р.Л. Добрушина* и *С.И. Самойленко*. М.: Мир, 1976. 596 с.

9. ГОСТ34.12—2018. Информационная технология. Криптографическая защита информации. Блочные шифры. М.: Стандартинформ, 2018 17 с.

10. *Крит А.А. Кораблев Е.Д.* Реализация однопроходных псевдослучайных последовательностей с помощью регистра сдвига с линейной обратной связью методом Галуа // Информационные техно-

логии и прикладная математика: сб. статей. Арзамас, 2023. С. 56–61.

11. The On Line Encyclopedia of Integer Sequences [Электронный ресурс]. URL: https://oeis.org/A008330 (дата обращения: 25.11.2024).

12. *Купаев Е.М. Федосенко Ю.С. Ямпурин Н.П. Логинов В.И.* Повышение криптостойкости алгоритмов шифрования на основе идеи Баттиста Порта // Всероссийская конференция с международным участием «Радиоэлектронные устройства и системы для инфокоммуникационных технологий» (REDS 2020). Москва, 2020. С. 275–278.

13. *Ключев А.Г. Логинов В.И. Федосенко Ю.С.* Методы кодирования информации для аппаратуры передачи конфиденциальных данных // Труды 22 го международного научно промышленного форума «Великие реки 2020». 2020. Вып. 9.

14. *Кораблев Е.Д. Крит А.А.* Реализация однопроходных псевдослучайных последовательностей линейным конгруэнтным методом // Информационные технологии и прикладная математика: сб. статей. Арзамас, 2023. С. 51–55.

15. *Кнут Д.Э.* Искусство программирования. Том 2. Получисленные алгоритмы. М.: Вильямс, 2007. 832 с.

16. Грушин П.И., Логинов В.И. Проектирование полосового фильтра с минимальными требованиями к реализации для подавления помех в ближней зоне / П. И. Грушин, // Радиотехнические и телекоммуникационные системы. 2012. № 4. С. 4–9.

Поступила 2 декабря 2024 г.

English

THE USE OF HAMMING CODES IN THE COMMUNICATION CHANNEL WITH DYNAMIC KEY CHANGE FOR CREW-FREE NAVIGATION

Nikolay Petrovich Yampurin — Grand Dr. in Engineering, Professor, Department "Design and Technology of Radio-Electronic Means", Arzamas branch[1] of Nizhny Novgorod State University.
E-mail: kitres@apingtu.edu.ru

Andrey Alexandrovich Krit — the Head of the Laboratory, Volga State University[2] of Water Transport.

Egor Denisovich Korablev — the Head of the Laboratory, Volga State University[2] of Water Transport.

Vyacheslav Ivanovich Loginov — PhD in Engineering, Associate Professor, Volga State University[2] of Water Transport.

Alla Sergeevna Stepanova — PhD in Engineering, Associate Professor, Volga State University[2] of Water Transport.

Yuri Semenovich Fedosenko — Grand Dr. in Engineering, Professor, the Head of the Department, Volga State University[2] of Water Transport.

[1]*Address:* 602264, Russian Federation, Nizhny Novgorod region, Arzamas, K. Marx str., 36.
[2]*Address:* 603950, Russian Federation, Nizhny Novgorod, Nesterov str., 5.

Abstract: The modern task of protecting information and preserving the integrity of data transmitted over wireless communication channels for controlling mobile objects and exchanging data highlights the need for effective information encoding methods. The control and communication systems of unmanned vessels and boats have to overcome the zone of electronic influence, which requires appropriate technical solutions. This article considers the possibility of using control over the integrity of a block bit sequence using the Hamming algorithm for a sequence formed as a result of the modified El Gamal algorithm and transmitted through communication channels subject to interference. The data processing in the system is analyzed to increase cryptographic strength, and a method is proposed to increase noise immunity.

Keywords: automation, gamming, wireless communication, crewless vessel control, linear pseudorandom sequence generator, redundant coding, Hamming algorithm, modified El Gamal algorithm.

References

1. Resolution MSC.428(98) [Electronic Source]: International Maritime Organization. URL: https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf (Access Date: 25.11.2024).

2. The first Russian unmanned research vessel departed from St. Petersburg to Sevastopol [Electronic resource]. Rossiyskaya Gazeta. 2022. URL: https://rg.ru/2022/08/30/reg-ufo/v-sevastopol-iz-peterburga-otpravilos-pervoe-rossijskoe-nauchno-issledovatelskoe-sudno-bespilotnik.html?ysclid=m7p53a9q4e446713553 (Access Date: 25.11.2024).

3. GOST R 21.1101 2020. Basic requirements for design and working documentation. Moscow: Standartinform, 2021. 12 p.

4. *Smart N.* Cryptography: a textbook; translated from English. Moscow: Tekhnosfera, 2006. 525 p.

5. *Slepovichev I.I.* Generators of pseudorandom numbers. Saratov: SSU, 2017. 118 p.

6. *Ferguson, N., Schneier, B.* Practical cryptography. Moscow: Williams, 2005. 424 p.

7. *Iampurin N.P., Krit A.A., Korablev E.D., Loginov V.I., Fedosenko I.S.* Implementation of an Encoding System with Dynamic Key Change Based on Pseudorandom Sequence Generators. 2024 Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO). Vyborg, Russian Federation, 2024. Pp. 1–5. DOI: 10.1109/SYNCHROINFO61835.2024.10617466.

8. *Peterson W., Weldon E.* Error-correcting codes. Edited by *R.L. Dobrushin* and *S.I. Samoylenko*. Moscow: Mir, 1976. 596 p.

9. GOST 34.12—2018. Information technology. Cryptographic protection of information. Block ciphers. Moscow: Standartinform, 2018. 17 p.

10. *Krit A.A., Korablev E.D.* Implementation of single-pass pseudorandom sequences using a linear feedback shift register with the Galois method. Informatsionnye tekhnologii i prikladnaya matematika: collection of articles. Arzamas, 2023. Pp. 56–61.

11. The On Line Encyclopedia of Integer Sequences [Electronic Source]. URL: https://oeis.org/A008330 (Access Date: 25.11.2024).

12. *Kupaev E.M., Fedosenko Yu.S., Yampurin N.P., Loginov V.I.* Enhancing the cryptographic strength of encryption algorithms based on the idea of Battista Porta. All-Russian Conference with International Participation "Radioelectronic Devices and Systems for Infocommunication Technologies" (REDS 2020). Moscow, 2020. Pp. 275–278.

13. *Klyuchev A.G., Loginov V.I., Fedosenko Yu.S.* Methods of information encoding for equipment transmitting confidential data. Proceedings of the 22nd International Scientific and Industrial Forum "Great Rivers 2020". 2020. Issue 9.

14. *Korablev E.D., Krit A.A.* Implementation of single-pass pseudorandom sequences using the linear congruential method. Informatsionnye tekhnologii i prikladnaya matematika: collection of articles. Arzamas, 2023. Pp. 51–55.

15. *Knuth D.E.* The Art of Computer Programming. Volume 2. Seminumerical Algorithms. Moscow: Williams, 2007. 832 p.

16. *Grushin P.I., Loginov V.I.* Design of a bandpass filter with minimal implementation requirements for near-field interference suppression. Radio and telecommunication systems. 2012. No. 4. Pp. 4–9.