https://doi.org/10.38013/2542-0542-2020-4-6-14
УДК.621.391

Комплексная защита информации в каналах «земля-борт»

Е. М. Ватрухин

Акционерное общество «Концерн ВКО «Алмаз – Антей», Москва, Российская Федерация

Рассмотрен комплексный метод защиты информации от канальных помех, имитации и ознакомления на основе ансамблей отечественных стохастических кодов, позволяющий сократить количество кодовых и аппаратных средств, применяемых при раздельном решении задач, по сравнению с реализацией единого алгоритма защиты и однократного введения избыточности. Представлены возможности стохастических кодов по реализации заданной гарантированной вероятности безошибочного декодирования в каналах с различными моделями ошибок, включая коротковолновые.

Ключевые слова: стохастические коды, защита от помех, имитостойкость, скрытность, аппаратура передачи данных, достоверность информации, вероятность необнаруженной ошибки, двоичный симметричный канал, q-ичный симметричный канал

Для цитирования: Ватрухин Е. М. Комплексная защита информации в каналах «земля-борт» // Вестник Концерна ВКО «Алмаз – Антей». 2020. № 4. С. 6–14. https://doi.org/10.38013/2542-0542-2020-4-6-14

For citation: Vatrukhin E. M. Integrated information protection in the ground-to-board channels // Vestnik Koncerna VKO “Almaz – Antey”. 2020. No. 4. P. 6–14. https://doi.org/10.38013/2542-0542-2020-4-6-14

Поступила 16.11.2020 *Отрецензирована* 07.12.2020 *Одобрена* 18.12.2020 *Опубликована* 30.12.2020

Введение

В статье «Новые возможности применения коротковолновой радиосвязи при решении боевой авиацией задач воздушно-космической обороны», опубликованной в № 2 за 2017 г. этого журнала, были рассмотрены вопросы новых информационных возможностей боевых летательных аппаратов за пределами радиогоризонта на базе технологий адаптивной коротковолновой радиосвязи, реализующих качество радиообмена, сравнимое с прямой видимостью.

Настоящий материал является продолжением темы в части одного из ключевых аспектов качества радиообмена, практически не затронутого в предыдущей статье, – возможности обеспечения комплексной защиты информации от всех возможных воздействий на нее в процессе передачи в каналах с непредсказуемыми характеристиками, в первую очередь коротковолновых. Тема статьи относится к вопросам сохранения целостности и скрытности информации в условиях помех и радиопротиводействия отечественной инновационной технологией ***комплексной защиты информации от помех, имитации и несанкционированного ознакомления, реализуемой стохастическими кодами с однократно вводимой избыточностью.***

Возможность широкого применения этой технологии стала результатом многолетних исследований отечественных ученых в теории передачи данных и защиты информации д.т.н. Л.М. Финка, д.т.н. В.И. Коржика, к.т.н. С.А. Осмоловского, д.т.н. Г.А. Кабатянского, д.т.н. И.Ю. Жукова, д.т.н. М.А. Иванова и др. [1–49]. Особая роль в использовании свойств универсальности помехозащитных случайных кодов, создании научного фундамента и реализации комплексной защиты информации с помощью стохастических преобразований принадлежит С.А. Осмоловскому (1946–2018), ученику одного из теоретиков теории связи д.т.н. Л.М. Финка.

Настоящей статьей автор хотел бы отдать дань уважения многолетнему труду товарища и однокурсника.

Основным фактором искажения информации всегда было и остается постоянное наличие помех в каналах связи, особенно в радиоканалах. Борьба с ними традиционно ведется применением обнаруживающих и/или исправляющих ошибки помехозащитных кодов, реализуемых, как правило, в аппаратуре передачи данных (АПД). Наибольшее распространение в сетях воздушной связи ВКС получила АПД типа Р-098 («Перевал»), эксплуатируемая в течение нескольких последних десятилетий.

Средства радиопротиводействия способны полностью или частично подавлять информационный обмен и/или изменять и навязывать ложную информацию. Защиту от таких воздействий обеспечивают специальные коды имитозащиты, реализуемые в отдельных устройствах. Нейтрализовать подавление обмена сосредоточенными шумовыми помехами можно программной перестройкой рабочей частоты (ППРЧ), изменением направления и ширины диаграмм излучения антенн и др.

Конфиденциальность информации, то есть защита от несанкционированного ознакомления, обеспечивается обычно специальной аппаратурой шифрования с использованием криптографических кодов. В ряде случаев в этой аппаратуре задачи сохранения конфиденциальности и имитозащиты решаются одновременно.

Все упомянутые функции защиты традиционно решаются независимо друг от друга схожими кодовыми конструкциями в различных типах аппаратуры, но имеют одну конечную цель – ***сохранение целостности*** информации. При этом нарушение конфиденциальности можно тоже рассматривать, в некотором смысле, как нарушение ее целостности-неприкосновенности для посторонних.

Все функции защиты обеспечиваются кодами, имеющими некоторую количественную избыточность, за счет чего формируются массивы так называемых «запрещенных» кодовых комбинаций, в которые под воздействием помех могут переходить несущие информацию «разрешенные» комбинации. Несколько отлично формируются криптографические коды сохранения скрытности, где главным отличительным фактором их конструкции является статистически равновероятная последовательность сигналов, передаваемая в канал и не зависящая от статистики появления отдельных букв в исходной шифруемой последовательности.

Интуитивное понимание влияния на верность принимаемых дискретных данных избыточного кодирования как инструмента повышения достоверности может дать аналогия с процессом конфиденциального разговора двух абонентов по телефонному каналу с большим зашумлением. В этом процессе «обмена данными» неразборчивые слова и даже отдельные буквы приходится повторять по нескольку раз по просьбе принимающего. Чем больше в итоге было уточнений и повторов, т.е. чем длиннее «кодовая конструкция – информационный блок», тем ближе принятая фраза к оригиналу, т.е. выше достоверность информации.

Можно предположить, что если абонент в условиях шумов способен хоть что-то принимать осмысленно, то возможно в конце концов добиться приема со 100 % достоверностью любой сложности фразы даже в тяжелейших помеховых условиях.

Аналогичный смысл этой фразы для дискретного канала содержится в одной из главных теорем информации К. Шеннона, которая утверждает, что, в принципе, можно получить сколь угодно большую достоверность принимаемой информации, если скорость ее передачи в канале меньше ее пропускной способности (т.е. наихудшего состояния слышимости – «пропускной способности» в приведенном примере, при котором еще существует возможность осмысленно принимать слова и после изменения которого в сторону снижения общение становится бесполезным из-за полного прекращения понимания смысла произнесенного).

Продолжая аналогию с телефонным разговором, также предположим, что в соседнем помещении некто хочет записать с помощью технических средств подслушанный разговор. Абонент такую возможность имеет в виду

и для предотвращения несанкционированной записи включает воду из крана, «стохастический», т.е. случайный, шум которой делает невозможным сохранить смысл разговора при записи. Это сравнение схоже с влиянием случайных сигналов на секретность данных при дальнейшем рассмотрении в статье понятия *q*-ичного симметричного канала.

Важнейшим параметром оценки эффективности обмена данными служит достоверность получаемой информации, которая зависит главным образом от вероятности ошибки, не обнаруживаемой конкретным защитным кодом ($p_{но}$). Необнаруженная ошибка – это, по сути, потеря информации, возникающая из-за превращения под воздействием помех «разрешенной» комбинации снова в «разрешенную», но соответствующую другому символу. Поэтому для уменьшения этой вероятности перехода желательно выбирать код, ***имеющий большой процент запрещенных кодовых комбинаций***, что ***возможно только при увеличении числа избыточных символов, а значит, увеличении длины кодовой комбинации.***

Из существующего множества избыточных кодов, которые обнаруживают и исправляют ошибки, на практике используется только очень малая их часть: коды Хэмминга, БЧХ, Рида – Соломона, сверточные и появившиеся недавно турбокоды [26]. Объясняется это в первую очередь тем, что распределение ошибок в реальных каналах связи таково, что ни один из этого множества кодов не позволяет обеспечить наперед заданную или ***гарантированную*** (в интересах повышения точности реализации конкретного информационного процесса) вероятность правильного приема информации в конкретном канале связи.

Все они создавались с ориентацией на некоторые математические модели каналов, которые лишь в очень грубых чертах описывают свойства реальных каналов связи [5, 8].

Наиболее часто применяемой при расчете параметров помехозащитного кода является модель некоего идеализированного канала, называемая «двоичным симметричным каналом» (ДСК), где ошибки имеют равные вероятности искажения «0» или «1».

Наиболее ярким образцом нестационарных каналов являются коротковолновые. Нестабильность их характеристик, а также наличие постоянных группирующихся помех не позволило до сегодняшнего дня создать их математическую модель приемлемой точности.

Начался поиск такой модели, желательно универсальной, под которую можно было бы создать код, который при заданных значениях n и k (где n – длина кодовой комбинации с избыточностью в битах, k – длина информационных бит в кодовой комбинации) обеспечивает в любых каналах связи некоторую ***гарантированную*** величину $p_{но}$. При этом желательно, чтобы при малых $p_{но}$ (порядка 10^{-9}–10^{-8}) потребителю практически не выдавалась бы ложная информация, а уменьшение скорости передачи (n/k) информации должно явиться сигналом для перехода к другому качеству канала связи.

Способ создания такого кода был разработан коллективом специалистов военной Академии связи в 70-х годах прошлого столетия во главе с д.т.н. Л.М. Финком [1].

В статье «Универсальное стохастическое кодирование в системах с решающей обратной связью» был математически обоснован ***способ получения заданной вероятности необнаруженной ошибки методом случайного кодирования с помощью стохастических преобразований***.

Под случайным кодированием, введенным в рассмотрение К. Шенноном для помехоустойчивого кодирования, понимают случайный выбор кодовых слов из множества возможных комбинаций с длиной, равной длине кода.

Полученная в этой работе формула (1) вероятности необнаруженной ошибки в любом канале настолько проста, что становится очевидной необходимость построения очень длинных кодов с большой избыточностью для получения малой $p_{но}$

$$p_{но} < 1/2^{n-k}. \quad (1)$$

Создание нового универсального кода было неразрывно связано с практической реализацией новой модели канала, так называемого $q(ку)$-ичного симметричного канала,

без которого новый код не имело смысла использовать, т. к. это, по сути, две стороны одной медали. С новой моделью появилась необходимость пересмотра некоторых традиционных взглядов на правила построения, кодирования и декодирования помехоустойчивых кодов.

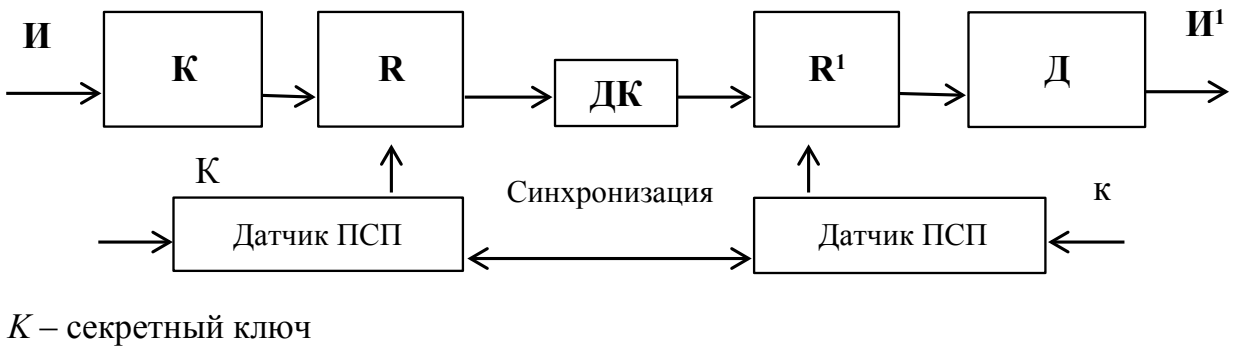
Понятие q-ичного симметричного канала, строго говоря, уже существовало, но только как математическая абстракция. Заслуга С.А. Осмоловского заключается в превращении абстракции в реальную модель и создании под нее помехоустойчивых случайных избыточных кодов, в дальнейшем называемых стохастическими, которые в q-ичном симметричном канале обладают рядом оригинальных свойств. Автор пришел к выводу, что ни один из классических кодов в рамках новой модели использовать не имеет смысла из-за потери их свойств, связанных с обнаружением, локализацией и исправлением ошибок: необходимо создать новый код, использующий факт наличия преобразованного дискретного канала. В реализованной им схеме (рис. 1) применено предложенное в [1] двойное последовательное преобразование: операций кодирования (кодер К) и прямого стохастического преобразования с использованием псевдослучайной последовательности на передающей стороне (R) и операций обратного стохастического преобразования и декодирования на приемной стороне. Совокупность из двух стохастических преобразователей R и R^{-1}, соединенных дискретным каналом связи ДК, образует q-ичный симметричный канал.

Двоичное сообщение разбивается на L-разрядные двоичные наборы – q-ичные символы, общее количество таких символов $q = 2^L$, nL-разрядная кодовая последовательность рассматривается как n-разрядный кодовый блок, состоящий из q-ичных символов, из которых k – информационные, а $n – k$ – избыточные.

В блоке кодирования К происходит преобразование информации И в двоичный n,k код с дальнейшим формированием в кодовые блоки длиной n q-ичных символов, где k символов – информационные. Затем информация поступает в блок прямого стохастического преобразования R, реализующий функцию рандомизации (*Random*) данных в двоичном дискретном канале (ДК) на случайных таблицах с дважды стохастическими матрицами переходов, блок обратного стохастического преобразования, реализующий функцию R^1, блок декодирования, в котором происходит обнаружение и исправление ошибок и выдача потребителю $И^1$ [2]. Рандомизация двоичных последовательностей служит также средством повышения точности описания исходов декодирования. Блоки R и R^1 осуществляют преобразование каждого q-ичного символа, при этом результат преобразования статистически не зависит от результатов преобразования других символов кодовой последовательности, что присуще криптографическим алгоритмам.

Свойство, которым теперь обладает преобразованный канал, заключается в равновероятности всех ситуаций, в которых происходят ошибки декодирования.

Таким образом, был практически создан дискретный канал новой модели, в котором



K – секретный ключ

Рис. 1. Схема передачи данных в q-ичном симметричном канале с применением стохастического кодирования

каждая ошибка L-разрядного q-ичного символа равна вероятности ошибки всех его остальных $(q-1)$ символов. При этом вероятность появления каждой ситуации, приводящей к ошибке декодирования, можно легко рассчитать, что позволило обеспечить наперед заданную вероятность правильного приема информации [2]. Автор обосновал длину q-ичного символа L равной 32 бит, при которой $p_{но}$ гарантирована не хуже 10^{-9}.

Современная тенденция к повышению точности обработки информационных потоков является объективной, что требует пересмотра требований к гарантированной вероятности ошибок в принимаемых данных после декодирования в сторону ее уменьшения до 10^{-9} с обычной сегодня, в большинстве случаев, 10^{-6}.

Такое повышение достоверности информации необходимо сегодня в системах управления при передаче координат целей высокоточным средствам поражения, при обработке и хранении больших объемов данных (big data), команд на применение спецоружия, управления БПЛА, для защиты информации при передаче открытых ключей в общей сетевой среде, идентификации «свой-чужой», передачи информации в декаметровом диапазоне волн и т.п.

В основу построения стохастических кодов с исправлением ошибок положен принцип локализации правильно принятой последовательности, использующий, в том числе, и некоторые положения современной теории линейных двоичных кодов [7].

Кратность исправляемых стохастическими кодами ошибок имеет вид $t = d - 2$ (где d – кодовое расстояние) [3]. Для большинства помехозащитных кодов $t = d - 1/2$.

Оптимальные параметры (n,k,q)-кодов для обеспечения максимальной скорости передачи n/k связаны с качеством канала (вероятностью искажения q-ичного символа p_q), максимальной кратностью исправляемых ошибок $d - 2$ и длиной кода n выражением $np_q = d - 2$.

Стохастические коды имеют тесную взаимосвязь между свойствами помехозащищенности и информационной скрытности, что позволяет при соответствующей реализации одновременно дополнительно обеспечивать секретность и контроль целостности передаваемой информации.

Практический метод такой реализации предложен д.т.н. М.А. Ивановым, специалистом в области защиты информации. Учитывая, что процедуры создания средств обеспечения секретности в нашем государстве жестко регламентированы и новые методы ее обеспечения должны быть специфицированы установленным порядком, предложено решение этих задач выполнять в соответствии с хорошо адаптируемыми под стохастические коды требованиями размеров блочных шифров стандарта ГОСТ Р 34.12-2015 «Информационная технология. Криптографическая защита информации. Блочные шифры».

Чтобы получить необходимые дополнительные функции, предложено реализовать в качестве блоков R и R^{-1} (рис. 1) многораундовые стохастические преобразования, а для генерации параметров стохастического преобразования – многовыходной генератор псевдослучайной последовательности (ГПСП), имеющий двухступенчатую конструкцию и специфицированный в ГОСТ Р 34.12-2015 для реализации шифрования методом гаммирования.

Реализация предложенной схемы передачи данных позволяет обеспечить ***универсальную защиту передаваемых данных единым алгоритмом с одноразовым внесением избыточности.*** При этом ***решается задача защиты от помех элементами стохастического помехоустойчивого кодирования, а секретность и целостность информации обеспечиваются за счет иных, криптографических по сути, схем прямого и обратного стохастического преобразования и требованиями к ГПСП, специфицированными в ГОСТ Р 34.12-2015 [5].***

Исправляющая способность стохастических кодов была испытана в рамках выполненной в Концерне ВКО ОКР «Арго» (автор выполнял функции Главного конструктора) на ансамбле из четырех стохастических кодов различной длины (8,2; 8,4; 16,7; 16,11), которые в коротковолновом канале обеспечили возможность использования адаптации к его

состояниям с повышением исправляющей способности различными длинами одновременно с сигнально-кодовыми конструкциями примененных КВ модемов.

При управлении авиацией, где зачастую необходим только режим однонаправленной передачи с требуемой гарантированной вероятностью, применение стохастических кодов, исправляющих ошибки, может иметь хорошую перспективу. Исправление ошибок, в принципе, способствует качественному улучшению сетевых технологий, прежде всего в части повышения их производительности, поскольку отказ от алгоритмических методов защиты информации методом переспроса при обнаружении ошибки и переход к кодовым методам исправления существенно повышает производительность дорогостоящих сетевых ресурсов. Кроме того, при исключении временных потерь на перезапрос увеличивается скорость обмена данными в радиосетях.

Ну и, безусловно, возможность программно реализовать одной кодовой конструкцией еще две важные функции защиты информации – имитостойкость и скрытность – является пока уникальной по критерию «эффективность–стоимость».

Практическое применение для работы в коротковолновом канале стохастические коды нашли в разработке специальной аппаратуры «Весна-4М».

Заключение

Использование стохастических преобразований в области комплексной защиты информации не имеет аналогов.

Достижением отечественной науки, признанным за рубежом [4, 49], можно считать создание новой модели q-ичного канала и ансамблей случайных стохастических кодов. Их наличие позволило получать высокие гарантированные достоверности с оптимальными для конкретного состояния канала скоростями обмена данными в широком классе каналов с непредсказуемыми параметрами, в частности коротковолнового диапазона.

В течение всего сеанса связи, когда характеристики таких каналов могут меняться неоднократно, применение ансамблей кодов обеспечивает устойчивый обмен за счет выбора из ансамбля оптимальной к каждому состоянию канала длины кода.

Использование q-ичного симметричного канала в этом диапазоне может стать лучшей альтернативой, причем «бесплатной», специальной процедуре перемежения, нашедшей широкое применение в коротковолновых модемах. Эта процедура предпринимается с целью преобразования групповых ошибок (пакетов ошибок) в одиночные ошибки, поскольку пакеты ошибок с большой вероятностью рассыпаются на одиночные ошибки.

Теми же кодовыми конструкциями при необходимости обеспечивается секретность информации.

Стохастические коды могут занять свое место для универсальной защиты информации с минимальными затратами в перспективных системах управления ВКС, гражданской авиации, включая радиоканалы управления пилотируемыми и особенно беспилотными летательными аппаратами, где необходим высокий уровень защиты от всех воздействий без применения шифрующей аппаратуры [6, 50].

Они эффективны для защиты информации в любых каналах обмена данными, при их хранении в памяти ЭВМ, для защиты от перехвата и дешифровки трафика в локальных вычислительных сетях [50], а также при обращении информации на разных видах носителей.

Список литературы

1. Коржик В.И., Осмоловский С.А., Финк Л.М. Универсальное стохастическое кодирование в системах с решающей обратной связью // Проблемы передачи информации. 1974. Т. 10, вып. 4. С. 25–29.

2. Иванов М.А., Ковалев А.В., Мацук Н.А., Чугунков И.В. Стохастические методы и средства защиты информации в компьютерных системах и сетях / Под ред. д.т.н. И.Ю. Жукова. М.: Кудиц пресс, 2009. 602 с.

3. Осмоловский С.А. Стохастическая информатика: инновации в информационных системах. Монография. М.: Горячая линия-Телеком, 2012.

4. Torleiv Klove, Korzhik V.I. Error Detecting Codes.General Theory and Their Application

in Feedback Communication System. Springer, 1995. 249 p. (разд. 1.4, 4.2).

5. Иванов М.А. Способ обеспечения универсальной защиты информации, пересылаемой по каналу связи // Вопросы кибербезопасности. 2019. № 3 (31). С. 45–50.

6. Мальцев Г.Н. Помехоустойчивость и скрытность передачи информации по радиоканалам на основе комбинированного случайного кодирования // Кодирование и передача информации. 2015. С. 82–89.

7. Моисеенков И. Основы безопасности компьютерных систем // Компьютер Пресс. 1991. № 10. С. 19–24; № 11. С. 7–21.

8. Финк Л.М. Теория передачи дискретных сообщений. М.: Советское Радио, 1970. 728 с.

9. Иванов М.А., Чугунков И.В. Криптографические методы защиты информации в компьютерных системах и сетях. Учебное пособие / Под ред. М.А. Иванова. М.: НИЯУ МИФИ, 2012. 400 с.

10. Осмоловский С.А. Универсальная защита информации: прецизионная защита информации. Монография. Издательский дом «Сталинград», 2014. 266 с.

11. Осмоловский С.А. Способ передачи и комплексной защиты информации. Патент РФ № 2367007, приоритет 20.08.2007. Решение о выдаче патента от 18.03.2009.

12. Осмоловский С.А. Построение и характеристики стохастических кодов, исправляющих ошибки // Вопросы радиоэлектроники. Серия общетехническая. 1980 (1981). Вып. 13/2. С. 136–146.

13. Осмоловский С.А. Стохастические методы передачи данных. М.: Радио и связь, 1991.

14. Осмоловский С.А. Стохастические методы защиты информации. М.: Радио и связь, 1995. С. 42–53.

15. Жуков И.Ю., Иванов М.А., Осмоловский С.А. Принципы построения генераторов псевдослучайных кодов, используемых при построении стойких криптоалгоритмов // Проблемы информационной безопасности. Компьютерные системы. 2001. № 1. С. 27–44.

16. Осмоловский С.А. Стохастическая информатика // Радиоэлектроника и управление. 2003. № 10–12.

17. Осмоловский С.А. Способ блочного шифрования информации. Патент России № 2266622. Заявка на патент РФ № 2004108916/09 (009857), приоритет 29.03.2004.

18. Осмоловский С.А. Способ генерации случайных чисел. Патент России № 2246129. Заявка на патент РФ № 2003100491/09 (000765), приоритет 13.01.2003.

19. Осмоловский С.А. Алгоритмы декодирования и свойства стохастических кодов с исправлением ошибок // Техника средств связи. Сер. ТПС. 1984. Вып. 4. С. 96–109.

20. Осмоловский С.А. Устройство для коррекции ошибок в блоках памяти. Авторское свидетельство СССР № 1086460, приоритет 16.07.1982, опубликовано 15.04.84, бюллетень № 14.

21. Осмоловский С.А. Стохастические коды, исправляющие ошибки с гарантированной точностью // Системы и средства связи, телевидения и радиовещания. 2001. № 2, 3. С. 15–24.

22. Осмоловский С.А. Помехоустойчивое кодирование: кризис и пути выхода из него // Вестник РУДН. Серия Прикладная и компьютерная математика. 2004. Т. 3, № 1. С. 161–169.

23. Осмоловский С.А. О возможности универсальной защиты информации стохастическими кодами // Вестник РУДН. Серия Прикладная и компьютерная математика. 2004. Т. 3, № 1. С. 170–177.

24. Осмоловский С.А. Стохастические технологии в информационно-телекоммуникационных системах: цели и ожидаемые результаты применения // Вестник РУДН. Серия Прикладная и компьютерная математика. 2005. Т. 4, № 1. С. 179–190.

25. Осмоловский С.А. Корректирующие коды для систем с гарантированными характеристиками и алгоритмом декодирования на основе предварительной локализации правильно принятых символов // Системы и средства связи, телевидения и радиовещания. 2006. № 1, 2. С. 65–70.

26. Осмоловский С.А. Турбокоды со случайным перемежением и стохастические коды с исправлением ошибок: общие и отличающиеся черты и свойства // Системы и средства связи, телевидения и радиовещания. 2006. № 1, 2. С. 71–75.

27. Осмоловский С.А. Общие принципы построения, свойства и возможности стохастических кодов // Системы и средства связи,

телевидения и радиовещания. 2006. № 1, 2. С. 65–70.
28. Осмоловский С.А. Информационные технологии защиты информации стохастическими кодами с исправлением ошибок // Труды VII международной конференции ICINASTe-2001, Минск, 2001. Т. 3. С. 15–22.
29. Осмоловский С.А. Абсолютная секретность по Шеннону — подход к реализации // Сборник научных трудов научной сессии МИФИ-2002. Т. 12.
30. Осмоловский С.А. Стохастическое помехоустойчивое кодирование как средство обобщения и решения задач помехоустойчивости и секретности в постановке Шеннона // Сборник научных трудов научной сессии МИФИ-2002. Т. 12.
31. Осмоловский С.А. О возможности защитить информацию от всех видов воздействий в рамках одного алгоритма // Труды IV Международного научного семинара. Информационные сети, системы и технологии. Москва, 16–19 сентября 2003 г.
32. Осмоловский С.А. Новое поколение программных средств стохастической защиты информации // Труды Пятого Всероссийского симпозиума по прикладной и промышленной математике, Кисловодск, 2–8 мая 2004 г.
33. Осмоловский С.А. Стохастическая информатика как новое направление в прикладной информатике // Труды V Международного семинара. Информационные сети, системы и технологии. Москва, 26–27 октября 2004 г.
34. Осмоловский С.А. Стохастическая информатика // Труды V Международного семинара «Информационные сети, системы и технологии». Москва, 26–27 октября 2004 г.
35. Осмоловский С.А., Скворцов В.Д. Исследование свойств программной реализации методов стохастической защиты // Труды V Международного семинара «Информационные сети, системы и технологии». Москва, 26–27 октября 2004 г.
36. Осмоловский С.А. Искусственные стохастические информационные системы: цели и порядок применения // Проблемы и методы информатики. II Научная сессия ИПИ РАН. Тезисы докладов. М.: ИПИ РАН, 2005. С. 116–119.
37. Осмоловский С.А. Новые задачи, которые можно решать только стохастическими методами // Материалы 6-го Всероссийского симпозиума по прикладной и промышленной математике (весенняя сессия). Санкт-Петербург, 3–7 мая 2005 г. СПб.: Редакция журнала ОПиПМ. С. 171–172.
38. Осмоловский С.А. Стохастические методы защиты информации: отличительные черты // Материалы 6-го Всероссийского симпозиума по прикладной и промышленной математике (весенняя сессия). Санкт-Петербург, 3–7 мая 2005 г. СПб.: Редакция журнала ОПиПМ. С. 172–173.
39. Осмоловский С.А. Стохастическое преобразование как ансамбль шифров // Материалы 6-го Всероссийского симпозиума по прикладной и промышленной математике (весенняя сессия), Санкт-Петербург, 3–7 мая 2005 г. СПб.: Редакция журнала .ОПиПМ. С. 173–174.
40. Осмоловский С.А. Стохастическое кодирование с исправлением ошибок как прорывная технология в области защиты информации // Материалы 12-й Всероссийской школы-коллоквиума по стохастическим методам (осенняя сессия), Сочи, 1–7 октября 2005 г. СПб.: Редакция журнала ОПиПМ. Т. 12. Вып. 3. С. 675–676.
41. Осмоловский С.А., Першов А.Н. Создание конкурентоспособной продукции в сфере телекоммуникаций за счет использования отечественных информационных технологий // Материалы Международной научной конференции МКИССиТ-2006. Информационные сети, системы и технологии. Санкт-Петербург, 30 октября — 2 ноября 2006 г. С. 11–13.
42. Осмоловский С.А. Стохастическая комплексная защита информации как средство создания нового поколения телекоммуникаций // Материалы Международной научной конференции МКИССиТ-2006. Информационные сети, системы и технологии. Санкт-Петербург, 30 октября — 2 ноября 2006. С. 42–44.
43. Осмоловский С.А. О пропускной способности произвольного канала связи // Материалы 14-й Всероссийской школы-коллоквиума по стохастическим методам (осенняя сессия). Сочи, 29 сентября — 7 октября 2007 г. СПб.:

Редакция журнала ОПиПМ. Т. 13. Вып. 4. С. 735–737.
44. Kabatiansky G., Osmolovsky S. On decoding of interleaving codes // Proceedings of the Workshop .Coding theory days in St. Petersburg.. Saint-Petersburg, Russia, October 6–19, 2008. P. 22–26.
45. Осмоловский С.А. Способ защиты информации в радио и локальной вычислительной сети. Патент России № 2266621. Заявка на патент Российской Федерации № 2004108917/09 (009958), приоритет 29.03.2004.
46. Осмоловский С.А. Способ адаптивной передачи информации. Патент России № 2264647. Заявка на патент РФ № 2004108918/09(009859), приоритет 29.03.2004.
47. Осмоловский С.А. Способ комплексной защиты информации. Патент России № 2292122. Заявка на патент РФ № 2005113925/09(016013).
48. Осмоловский С.А. Универсальный способ передачи информации с контролируемыми параметрами. Патент России № 2319199. Заявка на патент РФ № 2006109371/09(010194), приоритет 27.03.2006.
49. Torleiv Klove. University of Bergen, Norway. Series on Coding Theory and Cryptology. Codes for Error Detecting. Ch. 2. World Scientific Publishing Co. Pte. Ltd. 2007.

Об авторе

Ватрухин Евгений Михайлович – кандидат технических наук, старший научный сотрудник научно-технического центра воздушно-космической обороны Акционерного общества «Концерн ВКО «Алмаз – Антей», Москва, Российская Федерация.
Область научных интересов: информационно-управляющие, телекоммуникационные, навигационные системы, защищенные системы, передача данных, радиосвязь.

Integrated information protection in the ground-to-board channels

E. M. Vatrukhin

“Almaz – Antey” Corporation, JSC, Moscow, Russian Federation

This paper considers an integrated method of information protection against channel interference, imitation and familiarization based on ensembles of domestic stochastic codes. In comparison with the use of a single protection algorithm and a single introduction of redundancy, the proposed method reduces the number of code and hardware tools used when problems are to be solved separately. The possibilities of stochastic codes for the implementation of a given guaranteed probability of error-free decoding in channels with various error models, including short-wave ones, are presented.

Keywords: stochastic codes, protection against interference, imitation resistance, secrecy, data transmission equipment, information reliability, probability of undetected error, binary symmetric channel, q-ary symmetric channel

Information about the author

Vatrukhin Evgeny Mikhailovich – Cand. Sci. (Engineering), Senior Researcher, Research Organization,“Almaz – Antey” Corporation, JSC, Moscow, Russian Federation.
Research interests: information management, telecommunication and navigation systems; guarded systems; data transmission; radio communications.