УДК: 004.056

МЕТОДИКА ИМИТОЗАЩИТЫ ДАННЫХ, ПЕРЕДАВАЕМЫХ ПО РАДИОКАНАЛАМ КОМПЛЕКСОВ С БЕСПИЛОТНЫМИ ЛЕТАТЕЛЬНЫМИ АППАРАТАМИ

METHODS FOR PROTECTING FROM IMITATION DATA TRANSMITTED OVER RADIO CHANNELS OF COMPLEXES WITH UNMANNED AERIAL VEHICLES

Ю.О. Глобин

Yu.O. Globin

Краснодарское высшее военное училище им. С.М. Штеменко

Особенностью современного вооруженного конфликта является массированное применение комплексов с беспилотными летательными аппаратами. Это позволяет выполнять поставленные разведывательные задачи с минимальным риском для личного состава. Успешность выполнения данных задач во многом зависит от совершенства организации управления и связи в применяемых комплексах, и уровнях защищенности радиоканалов передачи данных, подверженных воздействию как непреднамеренных, так и преднамеренных помех. Предложена методика имитозащиты данных, передаваемых по радиоканалам комплексов с беспилотными летательными аппаратами. Применение методики позволяет повысить, с одной стороны, скорость передачи «полезной» информации в режиме обнаружения имитации передаваемых данных, а с другой — исправляющие возможности применяемого помехоустойчивого кода в режиме отсутствия злоумышленника в канале связи.
Ключевые слова: комплексы с беспилотными летательными аппаратами, помехоустойчивое кодирование в радиоканалах робототехнических комплексов, блочные разделимые коды, сверточные коды, имитовставка, имитозащита.

The feature of modern armed conflicts is the massive use of complexes with unmanned aerial vehicles. This allows to perform assigned intelligence tasks with minimal risk of loss of personnel. The success of these tasks largely depends on the organization of control and communication in the complexes used and the radio data channels level of security that are exposed to both unintentional and intentional interferences. The method for protecting from imitation data transmitted over radio channels of complexes with unmanned aerial vehicles is proposed. The application of the method allows to increase, on the one hand, the speed of «useful» information transmission in the detection mode of transmitted data imitation, on the other hand, the correcting possibility of the applied error-correcting code in the mode of absence of an attacker in the communication channel.
Keywords: complexes with unmanned aerial vehicles, error correction coding, block separable codes, convolutional codes, massage authentication code, protection from imitation.

В комплексах с беспилотными летательными аппаратами (КБЛА) организуется несколько каналов связи, одним из которых является направление от беспилотного летательного аппарата (БПЛА) к пункту управления (ПУ). Оно включает в себя направление «вниз» командной радиолинии управления для передачи телеметрической информации о состоянии подсистем БпЛА, специальной аппаратуры и технических средств полезной нагрузки, а также квитанций о выполнении команд управления и высокоскоростную линию передачи данных от специальной аппаратуры и технических средств полезной нагрузки, размещенных на борту [1].

Канал связи может функционировать в различных частотных диапазонах, использовать различные режимы и сигнально-кодовые конструкции, специально адаптированные под тип и важность передаваемых данных. Особенностью является то, что передаваемые данные имеют большой объем, требуют широкой полосы частот для передачи и в связи с высокими скоростями и необходимостью передачи в режиме реального времени могут не подвергаться криптозащите даже на БпЛА ведомственного назначения. Вскрытие сигнально-частотных параметров радиолинии, а также получение доступа к передаваемым данным для злоумышленника является достаточно тривиальной задачей, так как чаще всего на борту БпЛА для передачи данных применяются всенаправленные антенны.

На основе вскрытых сигнально-частотных параметров радиолинии злоумышленник способен определить тип и структуру сигналов, вскрыть формат и структуру передаваемых данных, тип протокола и другие параметры системы передачи данных. Создаётся возможность подмены данных путем формирования имитирующей помехи, прицельной по частоте и структуре сигнала, а также по структуре и формату передаваемых данных.

Применяемая в настоящее время для борьбы с имитационными воздействиями злоумышленника служебная информация — имитовставка [2] — вносит дополнительную избыточность в передаваемые данные, тем самым снижая скорость передачи «полезной» информации (под «полезной» информацией понимаются сведения, полученные специальной аппаратурой и передаваемые на ПУ, без учета служебной информации, например, заголовков пакетов, кадров, имитовставок и пр.). Это приводит к задержкам доведения разведданных, снижению оперативности принятия решений.

Вопросы защиты данных от имитации злоумышленником, передаваемых по радиоканалам КБЛА, исследовались А.В. Ананьевым [3], Д.В. Самойленко, О.А. Финько [4–5], С.В. Дворниковым (физический уровень) [6–7], И.Н. Оковым [8]. Несмотря на множество разработок в этой области, основным способом имитозащиты передаваемых данных в КБЛА является применение имитовставки вносящей дополнительную избыточность.

Развитием идей профессора О.А. Финько [9–11] стал разработанный способ имитозащиты данных, передаваемых с использованием блочных разделимых кодов [12], который обладает рядом преимуществ относительно стандартного решения. Также разработан способ обеспечения имитоустойчивой передачи данных при использовании сверточных кодов [13]. Главными особенностями разработанных способов является возможность обнаружения имитонавязывания ложных данных злоумышленником за счет обнаруживающих свойств помехоустойчивого кода. Факт имитонавязывания при этом обнаруживается как и любая помеха в канале связи, приводящая к ошибкам в данных на канальном уровне (однако восстановить целостность передаваемых данных при этом невозможно). Криптографическая стойкость полученных решений при этом как правило ниже чем стойкость, которую позволяет получить имитовставка. Однако целесообразность использования предложенных решений «оправдывает» одновременное сочетание:

– возможности «фильтрации» ложных пакетов ещё до того, как они поступят в обработку на уровне представления модели OSI, предотвращая тем самым реализацию противником угрозы безопасности «отказ в обслуживании»;

– реализации «стандартных» функций защиты от случайных помех без внесения дополнительных (помимо избыточных символов помехоустойчивого кода) служебных данных. При этом защита пользовательской информации продолжает осуществляется стандартными криптографическими методами на уровне представления.

Таким образом, ставится задача разработки методики имитозащиты данных, передаваемых

по радиоканалам КБЛА, применение которой позволит повысить, с одной стороны, скорость передачи «полезной» информации в режиме обнаружения имитации передаваемых данных при сохранении требуемого уровня имитоустойчивости системы передачи данных, с другой стороны — корректирующие возможности применяемого кода в режиме отсутствия злоумышленника в канале связи.

Исходными данными методики будут являться:

M — данные, подлежащие передаче с БПЛА на ПУ, представляющие в общем виде набор нулей и единиц;

$G = \{G_1, G_2\}$ — множество используемых при передаче данных помехоустойчивых кодов (далее — ПК), состоящее из подмножества G_1 блочных кодов, имеющих параметры n (количество символов в кодовом слове), k (количество информационных символов в кодовом слове) и d (минимальное кодовое расстояние), и подмножества G_2 непрерывных кодов, имеющих параметры h (количество применяемых кодеров), $g_1, g_2, \ldots g_h$ (производящие многочлены кодеров);

I — имитовставка, представляющая собой специальный набор символов, добавляемый к сообщению и предназначенный для обеспечения его целостности и аутентификации источника, имеющая параметр r (размер имитовставки);

$X = \{X_1, X_2\}$ — множество ключей, состоящее из двух подмножеств, где X_1 — подмножество ключей, используемых для вычисления имитовставки, X_2 — подмножество ключей, используемых для функционирования разработанного способа.

На рис. 1 представлена обобщенная структура разработанной методики. В целях ее эффективного использования представлено пошаговое описание основных этапов методики.

Шаг 1. Определяются требования действующих на этапе формирования проектной документации КБЛА нормативно-правовых актов по обеспечению помехоустойчивости и имитоустойчивости передачи данных по радиоканалам.

Шаг 2. Выполняется анализ условий функционирования КБЛА (дальность применения, возможная помеховая обстановка, применяемые средства радиоэлектронного подавления злоу-

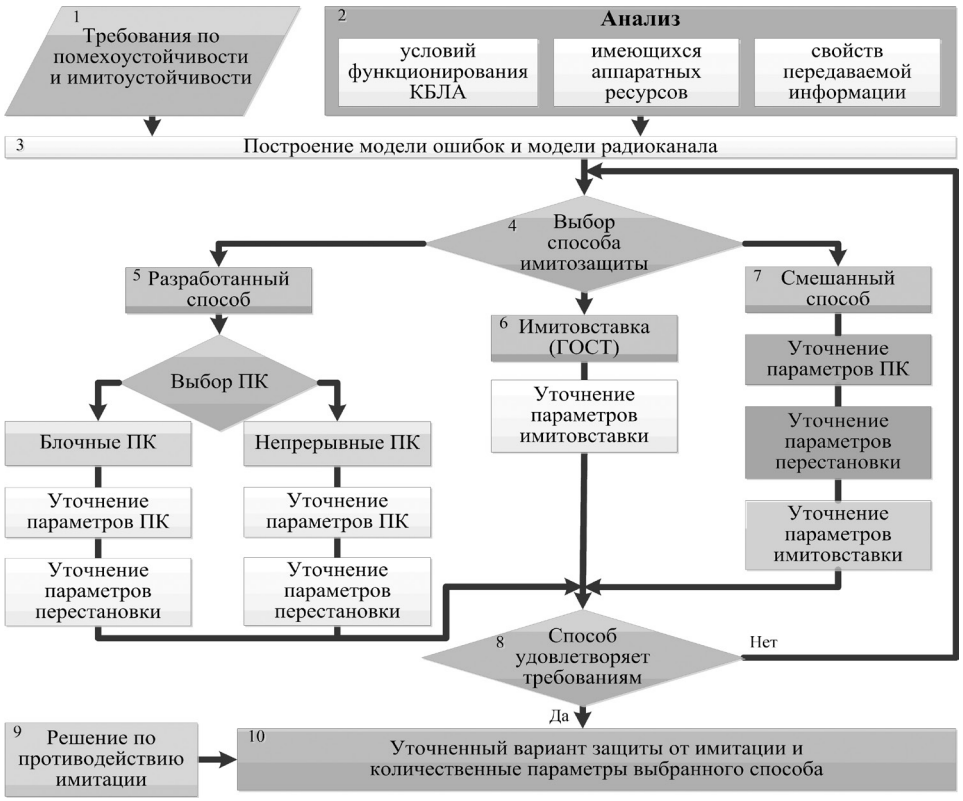


Рис. 1. Общая структура методики имитозащиты данных, передаваемых по радиоканалам КБЛА

мышленника), имеющихся аппаратных ресурсов (аппаратура приема/передачи данных, используемые радиоканалы, наличие элементной базы для реализации процедур имитозащиты), свойств передаваемой информации (общий объем передаваемых данных, размер кадра передаваемых данных, релевантность передаваемых данных).

Шаг 3. На основе выпо лненного анализа разрабатывается модель ошибок и модель используемого радиоканала в КБЛА с целью определения наиболее применимых классов ПК и их параметров.

Шаг 4. Выбирается в зависимости от свойств передаваемой информации и требований по имитоустойчивости наиболее подходящий способ имитозащиты.

В частности, если требуется передать небольшой объем данных, подходящим способом имитозащиты будет использование имитовставки, так как для разработанного способа требуется набор определенной статистики передаваемых кадров. По показателю имитостойкости также преимущество имеет имитовставка, так как вероятность вскрытия имитовставки $P_{\text{вскрытия}}$ методом полного перебора определяется ее длиной и составляет (грубо) $P_{\text{вскрытия}} = 2^{-r}$.

В разработанном способе, с одной стороны, вероятность вскрытия определяется перестановкой, имеющей сложность $n!$. С другой стороны, общее количество возможных комбинаций последовательностей на входе и выходе перестановки составляет 2^n, а количество разрешенных комбинаций в соответствии с применяемым ПК составляет 2^k. Таким образом, при случайном подборе информационных последовательностей вероятность подбора разрешенной кодовой комбинации составляет (грубо): $P_{\text{подбора}} = 2^{k-n}$, что может быть несколько выше (хуже), чем вероятность вскрытия имитовставки. Однако данная уязвимость не является критичной, так как предназначение предлагаемого решения — грубая «фильтрация» данных с признаками преднамеренного нарушения целостности на канальном уровне, имеющая целью предотвращение реализации угрозы безопасности информации «отказ в обслуживании», например, вследствии «зависания» шифратора, реализующего свои функции на уровне представления.

Разработанный способ в сравнении с применением имитовставки имеет преимущество в скорости передачи «полезной» информации и помехоустойчивости передачи данных, что обуславливает целесообразность выбора на данном шаге разработанного способа при условии выполнения требований по имитоустойчивости. В противном случае используется имитовставка. Кроме того, предлагается смешанный способ имитозащиты, при котором к разработанному способу добавляется применение имитовставки, однако вычисляется она не для отдельных кадров передаваемых данных, а для совокупности кадров с целью уменьшения доли служебной информации, вносимой имитовставкой в передаваемые данные и для сохранения минимального уровня защищённости передаваемых данных, соответствующего уровню, обеспечивающим стандартным решением.

Шаг 5–7. В зависимости от выбранного способа реализуется один из шагов. При этом независимо от выбранного способа предполагается, что на данном шаге выполняется предварительный выбор параметров имитозащиты, имитационное моделирование системы передачи данных с выбранными параметрами и разработанной моделью радиоканала. При необходимости выполняется уточнение выбранных параметров. Обобщенные последовательности процедур, выполняемых при реализации каждого из способов, представлены на рис. 2–3.

Шаг 8. При выполнении заданных требований по помехоустойчивости и имитоустойчивости выбранный способ реализуется в системе передачи данных КБЛА, в противном случае происходит возвращение к шагу 4 для выбора альтернативного способа имитозащиты.

Шаг 9. В зависимости от имеющихся аппаратных ресурсов и решаемых задач выбираются возможные варианты решения по противодействию имитации, например, смена радиоканала, передача данных с другого БпЛА, прерывание связи и др.

Шаг 10. Формируется уточненный вариант защиты от имитации и количественные параметры выбранного способа.

Выигрыш разработанного способа имитозащиты в сравнении с имитовставкой по помехоустойчивости системы передачи данных

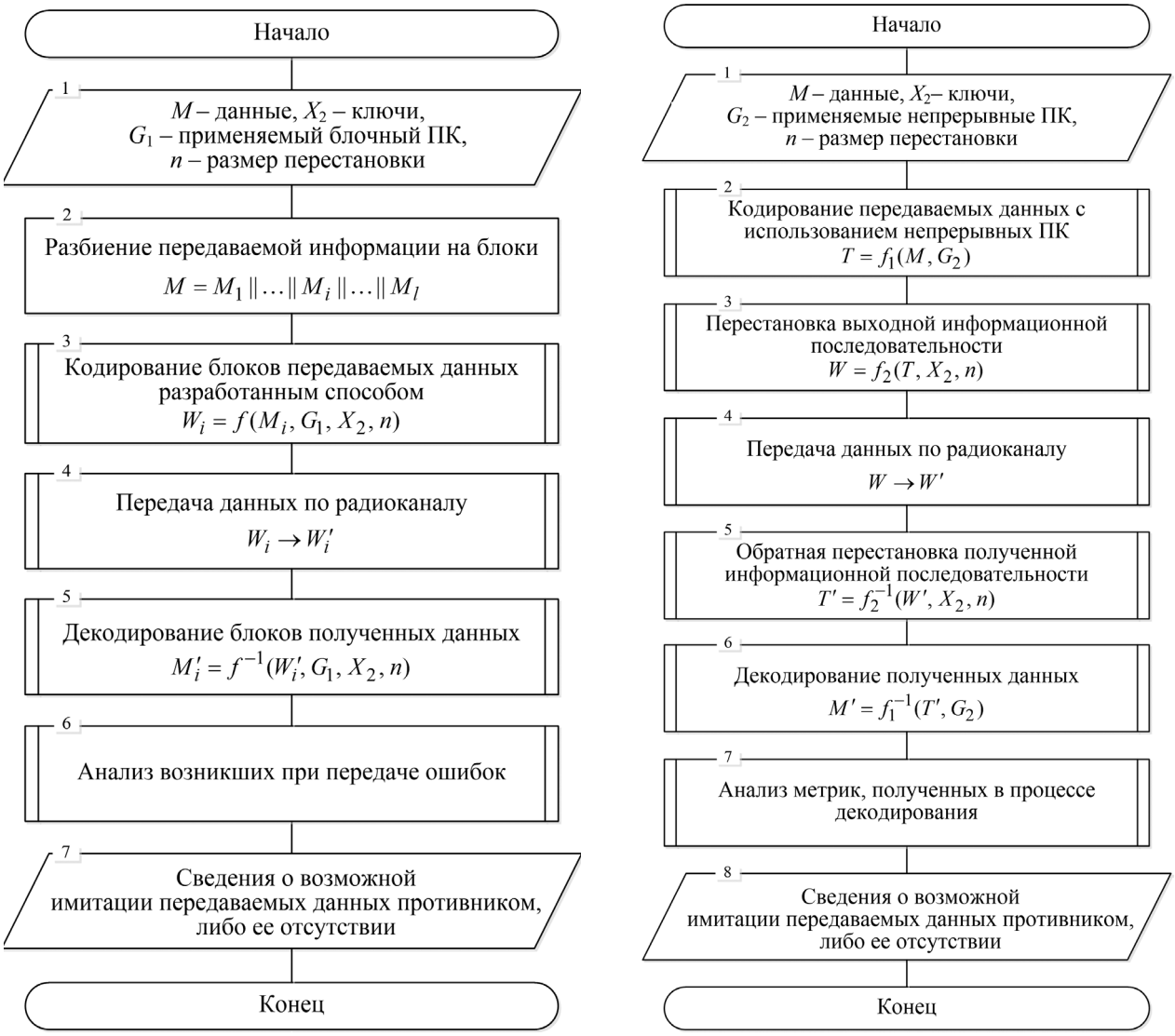


Рис. 2. Последовательность процедур, реализующих разработанный способ с блочными (а) и непрерывными (б) ПК

оценивается по вероятности достоверного исправления ошибок, возникших при передаче. При этом предполагается, что ошибка в каждом бите независима от других битовых ошибок, следовательно, возникшие ошибки имеют биномиальное распределение. Оценка выигрыша по данному показателю представлена на рис. 4. Для примера взяты циклические помехоустойчивые коды с указанными параметрами. Предполагается, что с кодом 2 и кодом 4 имитозащита реализуется использованием имитовставки, имеющей длину $r = 32$ бита. В коде 1 и коде 3 реализован разработанный способ, а биты, зарезервированные для размещения имитовставки, использованы в целях для увеличения избыточности ПК.

На рис. 5 представлены результаты анализа зависимости условной скорости передачи информации от размера кадра, которые свидетельствуют о преимуществах разработанного способа в сравнении с применением имитовставки. Сравнение выполнено с двумя часто применяемыми размерами имитовставки. Предполагается, что применяется один и тот же ПК, но вместо битов имитовставки передаются биты, содержащие «полезную» информацию.

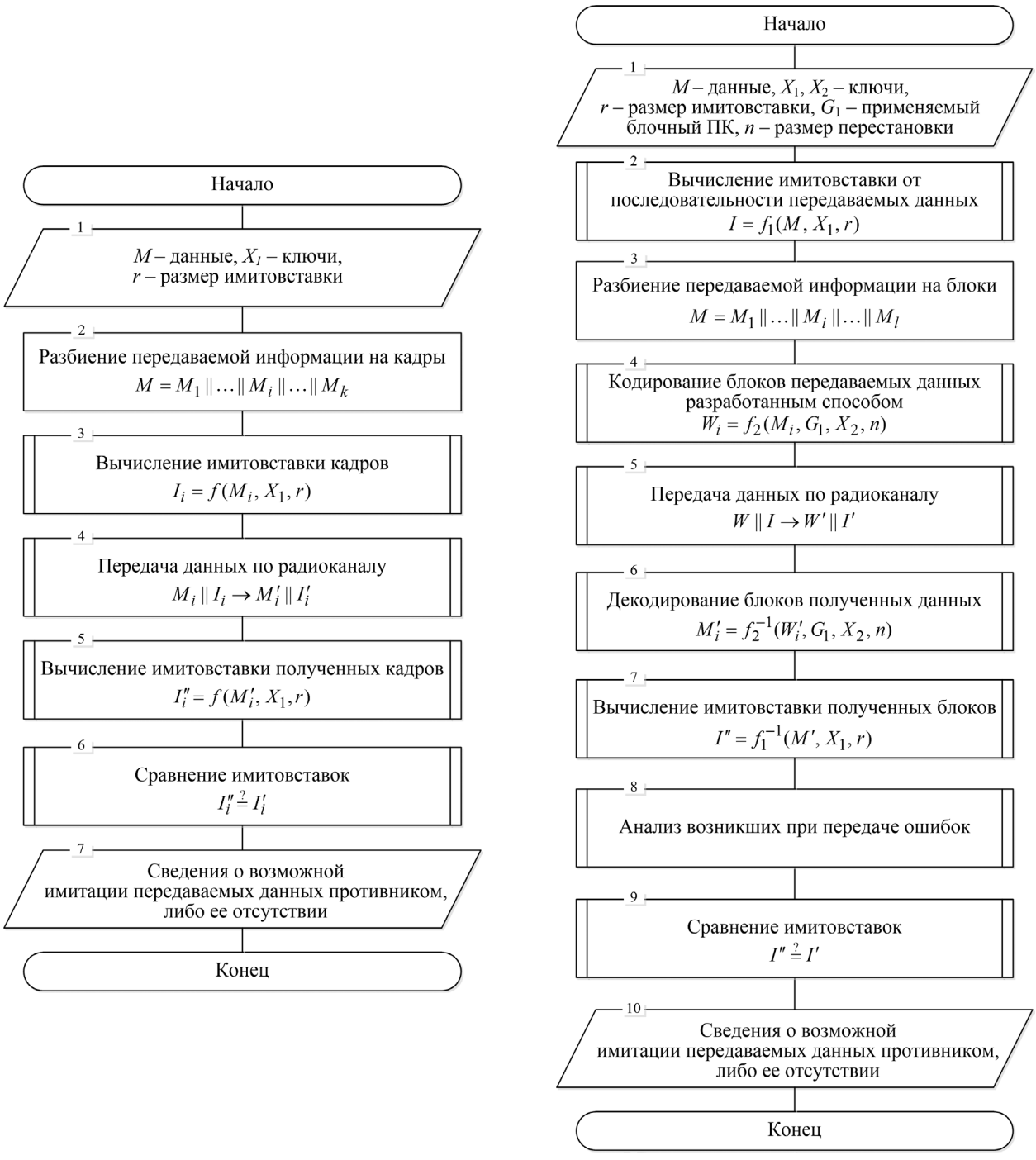
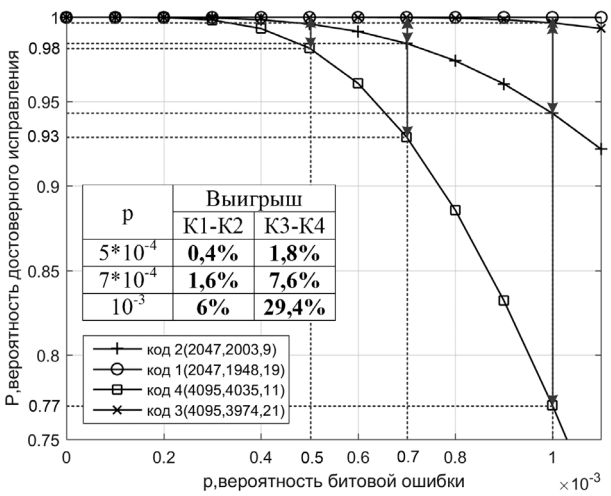
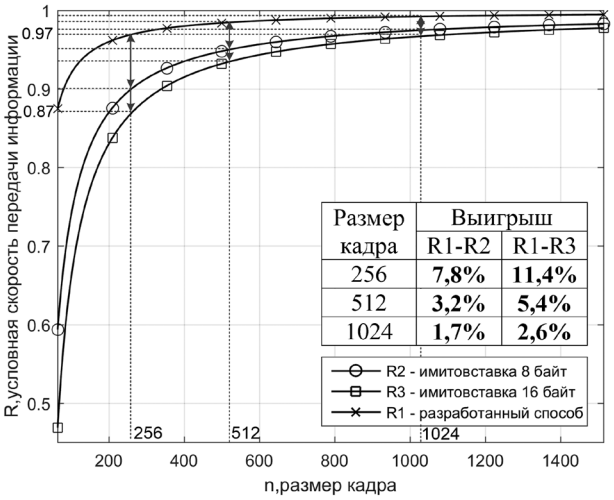


Рис. 3. Последовательность процедур, реализующих способ с применением имитовставки (а) и смешанный способ (б)



p	Выигрыш	
	К1-К2	К3-К4
$5*10^{-4}$	**0,4%**	**1,8%**
$7*10^{-4}$	**1,6%**	**7,6%**
10^{-3}	**6%**	**29,4%**

Рис. 4. Зависимости вероятностей достоверного исправления ошибки от вероятности битовой ошибки для различных кодовых конструкций (К1 — код 1, К2 — код 2, К3 — код 3, К4 — код 4)



Размер кадра	Выигрыш	
	R1-R2	R1-R3
256	**7,8%**	**11,4%**
512	**3,2%**	**5,4%**
1024	**1,7%**	**2,6%**

Рис. 5. Зависимость условной скорости передачи информации от размера кадра

Вывод

Представленное решение позволяет повысить скорость передачи «полезной» информации в режиме обнаружения имитации передаваемых данных при сохранении требуемой имитостойкости системы передачи данных, а в режиме отсутствия злоумышленника в канале связи, повысить корректирующие способности применяемого кода. Методика разработана в интересах должностных лиц, проектирующих перспективные КБЛА ведомственного назначения.

Литература

1. Макаренко С.И. Анализ средств и способов противодействия беспилотным летательным аппаратам. Часть 3. Радиоэлектронное подавление систем навигации и радиосвязи // Системы управления, связи и безопасности. 2020. № 2. С. 101–175.

2. Основы криптографии: учебное пособие / Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. — М.: Гелиос АРВ. 2001. 480 с.

3. Ананьев А.В., Змий Б.Ф., Кащенко Г.А. Модернизация бортовых приемо-передающих систем беспилотных летательных аппаратов на основе эволюционного подхода // Радиотехника. 2016. № 8. С. 46–49.

4. Самойленко Д.В., Финько О.А. Имитоустойчивая передача данных в защищенных системах однонаправленной связи на основе полиномиальных классов вычетов // Нелинейный мир. 2013. Т. 11. № 9. С. 647–658.

5. Самойленко Д.В., Финько О.А. Помехоустойчивая передача данных в радиоканалах робототехнических комплексов на основе полиномиальных классов вычетов // Наукоемкие технологии в космических исследованиях Земли. 2016. Т. 8. № 3. С. 49–55.

6. Дворников С.В., Погорелов А.А., Дворников С.С., Иванов Р.В. Предложения по восстановлению сигналов в каналах управления беспилотных летательных аппаратов // Вопросы радиоэлектроники. Серия: Техника телевидения. 2020. № 1. С. 91–97.

7. Дворников С.В. Методика оценки имитоустойчивости каналов управления роботизированных устройств // Радиопромышленность. 2016. № 2. С. 64–69.

8. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. — М.: Солон-Пресс, 2017. 262 с.

9. Еремеев М.А., и др. Распределённая обработка и защита информации в группировке комплексов с беспилотными летательными

аппаратами // Теория и техника радиосвязи. 2017. № 4. С. 93–100.

10. Samoylenko D.V., Eremeev M.A., and others. A method of providing the integrity of information in the group of robotic engineering complexes based on crypt-code constructions // Automatic Control and Computer Sciences. 2017. Vol. 51. P. 965–971.

11. Eremeev M.A., Dichenko S.A., and others. Protection of Information from Imitation on the Basis of Crypt-Code Structures, Advances in Soft and Hard Computing. ACS 2018. Advances in Intelligent Systems and Computing. Vol. 889. Springer. Cham. 2019. P. 317–331.

12. Глобин Ю.О., Финько О.А. Способ обеспечения имитоустойчивой передачи информации по каналам связи // Наукоемкие технологии в космических исследованиях Земли. 2020. Т. 12. № 2. С. 30–43.

13. Глобин Ю.О. Защита данных от имитации в системах потокового вещания на основе непрерывных кодов // Студенческая наука для развития информационного общества: сборник материалов X Всероссийской науч.-техн. конференции с международным участием. Ч. 1. — Ставрополь: Изд-во СКФУ. 2019. С. 59–67.

References

1. Makarenko S.I. Counter Unmanned Aerial Vehicles. Part 3. Electronic Warfare against Navigation and Radio Connection Subsystems of Unmanned Aerial Vehicles. Systems of Control, Communication and Security. 2020. № 2. P. 101–175.

2. Alferov A.P., Zubov A.Yu., Kuz'min A.S., Cheremushkin A.V. Basics of Cryptography. — Moscow: Gelios ARV. 2001. 480 p.

3. Ananev A.V., Zmiy B.F., Kaschenko G.A. Upgrade onboard transceiver systems of unmanned aerial vehicles on the basis of the evolutional approach. Radiotekhnika. 2016. № 8. P. 46–49.

4. Samoylenko D.V., Finko O.A. Imitation proof data transmission in protected system of one-way communication by means of polynomial residue classes. Nonlinear World. 2013. Vol. 11. № 9. P. 647–658.

5. Samoylenko D.V., Finko O.A. Noise immunity of data transmission in a radio channel robotic complexes based on polynomial residue classes. H&ES Research. 2016. Vol. 8. № 3. P. 49–55.

6. Dvornikov S.V., Pogorelov A.A., Dvornikov S.S., Ivanov R.V. Proposals for restoring signals in control channels of unmanned aerial vehicles. Questions of radio-electronics, the TV equipment series. 2020. № 1. P. 91–97.

7. Dvornikov S.V. Procedure of evaluation of imitation stability of robotic devices control channels. Radio industry. 2016. № 2. P. 64–69.

8. Gribunin V.G., Okov I.N., Turincev I.V. Digital steganography. — M.: Solon-Press. 2017. 262 p.

9. Eremeev M.A.et al. Distributed processing and data protection in the group of complexes with unmanned aerial vehicles. Radio Communication Theory and Equipment. 2017. № 4. P. 93–100.

10. Samoylenko D.V., Eremeev M.A. et al. A method of providing the integrity of information in the group of robotic engineering complexes based on crypt-code constructions // Automatic Control and Computer Sciences. 2017. Vol. 51. P. 965–971.

11. Samoylenko D.V., Eremeev M.A., Dichenko S.A.et al. Protection of Information from Imitation on the Basis of Crypt-Code Structures, Advances in Soft and Hard Computing. ACS 2018. Advances in Intelligent Systems and Computing. Vol. 889. Springer. Cham. 2019. P. 317–331.

12. Globin Y.O., Finko O.A. The way of ensuring resistant to imitation transmission information via communication channels. H&ES Research. 2020. Vol. 12. № 2. P. 30–43.

13. Globin Y.O. Protection of data from imitation in streaming systems based on continuous codes. Student science for development of the information society: materials of X Russian scientific-technical conference with international participation. Part 1. — Stavropol': SKFU. 2019. P. 59–67.