МЕТОДИКА ОЦЕНКИ ЭФФЕКТИВНОСТИ ФУНКЦИОНИРОВАНИЯ АППАРАТУРЫ ПЕРЕДАЧИ ДАННЫХ

Овчаренко Михаил Вячеславович,
г. Ростов-на-Дону, Россия, prepod84@mail.ru

Аннотация. В статье рассматриваются этапы методики оценки эффективности функционирования аппаратуры передачи данных (АПД). На основе анализа функционирования АПД в условиях радиоэлектронной борьбы определена ее низкая имитостойкость к навязыванию ложной информации. Предложена методика оценки эффективности АПД, реализованной на алгоритмах имитостойкого сверточного кодирования. В результате имитационного моделирования получены новые научными результатами, позволяющие оценить выигрыш от применения алгоритмов имитостойкого кодирования по показателям: вероятность правильного приема и вероятность навязывания ложной информации. Практическая направленность заключается в возможности использования разработанного программного комплекса для оценки эффективности как существующей, так и перспективной АПД на этапах ее проектирования.

Ключевые слова: аппаратура передачи данных, имитостойкость, имитационное моделирование, методика.

Сведения об авторе: Овчаренко М.В., начальник службы – помощник начальника штаба в/ч 12628.

Аппаратура передачи данных (АПД) применяется в автоматизированных системах управления (АСУ) и предназначена для автоматизированного обмена информацией по каналам передачи данных, обеспечения радио и проводной телефонной связью с вышестоящим пунктом управления, с подчиненными подразделениями и взаимодействующими изделиями. Эффективность функционирования АСУ непосредственно зависит от помехозащищенности и имитостойкости АПД.

Анализ алгоритмов функционирования АПД [1], показал, что задача защиты АПД от имитационных помех, воздействующих на сигнальном и информационном уровнях в основном не решена [2]. Для решения данной задачи были предложены алгоритмы имитостойкого сверточного кодирования [3-5].

Методика оценки эффективности функционирования АПД, реализованной на алгоритмах имитостойкого сверточного кодирования, представлена следующими этапами:

выбор и обоснование показателей эффективности функционирования АПД;

построение имитационной модели, включая комплекс программных средств;

проведение имитационного моделирования;

оценка результатов, полученных в ходе моделирования;

разработка рекомендации по реализации полученных результатов при проектировании и разработке перспективной АПД.

Для моделирования отдельных процессов и подсистем, имеющих сложный характер поведения, используются технологии компьютерного имитационного моделирования. Имитационная модель – это формальное описание логики функционирования исследуемой системы и взаимодействия ее отдельных элементов во времени, учитывающее наиболее существенные причинно-следственные связи, присущие системе, и отражающее поведение моделируемого объекта во времени и пространстве [6].

Целесообразность применения имитационного моделирования АПД определяется следующими факторами:

характер протекающих в АПД процессов достаточно сложен и не позволяет описать эти процессы в единой аналитической форме;

требуется провести исследование новых ситуаций в системе;

требуется изучить модельное поведение системы в условиях, недоступных для исследователя.

Целью статьи является представление методики и результатов проведения имитационного моделирования перспективной АПД, реализованной на алгоритмах имитостойкого сверточного кодирования.

Алгоритм проведения имитационного моделирования представлен на рис. 1.

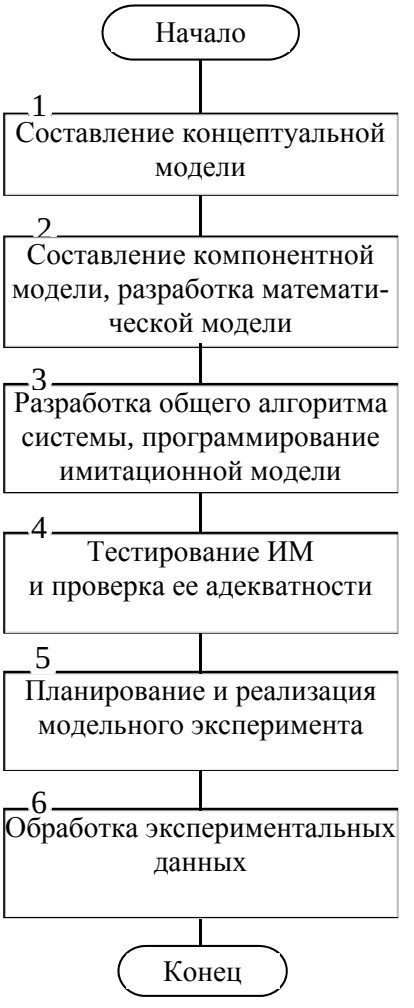

Рис. 1. Алгоритм проведения имитационного моделирования

Для проведения имитационного моделирования был разработан комплекс программ в среде программирования Delphi 7 [7], в частности, была разработана программа кодирования / декодирования информации в АПД при воздействии на канал связи различных кодовых комбинаций ошибок $Z_e = \{e_1 \ldots e_n\}$. Структурная схема имитационной модели представлена на рис. 2.

Рис. 2. Структурная схема имитационной модели

Исходными данными для моделирования являлись:

канал связи – двоичный симметричный канал, реализующий схему Бернулли;

порождающие многочлены для несистематического сверточного кодера: $G_1(X)=1+X+X^2$; $G_2(X)=1+X^2$ с параметрами кода: память кода L=3, полная длина кодового ограничения $l_п$=6, минимальное свободное расстояние d_{min}=5, скорость кода R=1/2;

объем криптограммы – 608 бит;

количество переданных криптограмм – 9107;

Общая математическая модель основывается на математическом описании способа имитостойкого кодирования и процесса формирования ошибок с биномиальным распределением.

Общий алгоритм следующий:

а) ввод файла и установка начальных параметров;

б) формирование ключевой информации;

в) имитостойкое сверточное кодирование;

г) имитация передачи по каналу связи;

д) декодирование;

е) изменение исходных параметров и параметров алгоритма;

ж) сбор результатов.

Программирование и отладка модели осуществлялась в среде объектно-ориентированного программирования Delphi 7.0 со встроенными процедурами тестирования

Главное меню программы (рис. 3) представлено вкладками:

«режим кодирования»;

«режим декодирования».

Предусмотрено два режима работы:

с шифрованием информации (режим имитостойкого сверточного кодирования);

без шифрования (режим сверточного кодирования).

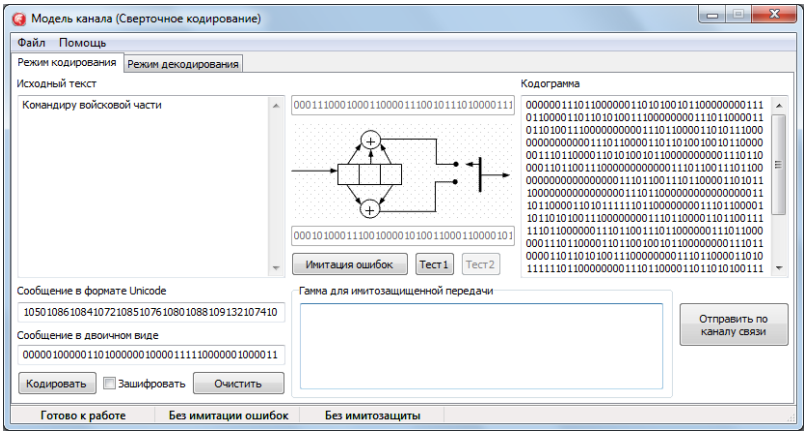

Рис. 3. Интерфейс программного средства

Работа программного средства в режиме имитостойкого сверточного кодирования обеспечивает:

ввод исходного текста сообщения;

отображение сообщения в формате Unicode;

отображение сообщения в двоичном виде;

выработка ключевой гаммы;

имитостойкое кодирование;

отображение результата кодирования.

Алгоритмы функционирования моделирующего программного средства базируются на принципах способа имитостойкого сверточного кодирования [3]. Основным требованием к программному средству имитационного моделирования является имитация ошибок канала связи. С этой целью в программном средстве реализован модуль генерации ошибок, позволяющий генерировать заданное количество ошибок или осуществить их полный перебор.

В рассмотренном режиме осуществляется сбор статистических данных по работе сверточного кодирования в режиме обнаружения и исправления ошибок.

Вторым этапом исследования является работа программы в режиме имитационного сверточного кодирования. В данном случае целью моделирования является сравнительный анализ влияния дополнительного режима шифрования на корректирующие свойства сверточного кода. Для решения данной задачи осуществлена имитация передачи криптограмм 9107 раз с полным перебором внесения ошибок e=(1÷4) и оценка их корреляции с криптограммами, полученными на первом этапе моделирования (в режиме сверточного кодирования).

Проверка адекватности, заключающаяся в доказательстве факта, что точность результатов, полученных по модели, будет не хуже точности расчетов, произведенных на основании экспериментальных данных, проводилось путем сравнительного анализа выходных данных программного средства с результатами, полученными с помощью ПО MS Excel.

При проверке непротиворечивости модели оценивались результаты при вариации величин важнейших параметров модели, включая их значения, приближенные к экстремальным.

Заключительный этап имитационного моделирования предусматривал вторичную обработку данных, на основе использования статистической обработки первичных данных и выработку информации, отражающую закономерности функционирования АПД, а также анализ и интерпретацию информации, полученной по результатам модельного эксперимента, в форме определенных выводов и рекомендаций.

Результаты эксперимента представлены в таблице 1.

Таблица 1

№ п\п	Тип эксперимента	Количество ошибок, e	Количество переданных криптограмм, N	Количество достоверно принятых криптограмм, $N_д$
1	Сверточное кодирование	1	156	154
2	Имитостойкое кодирование	1	156	154
3	Сверточное кодирование	2	1462	1378
4	Имитостойкое кодирование	2	1462	1375
5	Сверточное кодирование	3	4486	1689
6	Имитостойкое кодирование	3	4486	1692
7	Сверточное кодирование	4	9107	2173
8	Имитостойкое кодирование	4	9107	2178

Для подтверждения достоверности, полученных в ходе имитационного моделирования результатов, проведена оценка точности метода статистических испытаний [8] с использованием статистических функций MS Excel, позволившая определить нормальный закон распределения генеральной совокупности и рассчитать требуемый объем выборки $n_ф$=168 при значении доверительной надежности γ=0,95.

В рамках исследования статистических свойств имитостойкого сверточного кодирования проверялась гипотеза о том, что коэффициент корреляции между криптограммами, обработанными в режимах кодирования с обеспечением имитостойкости и без обеспечения имитостойкости, приближается к единице (рис. 4).

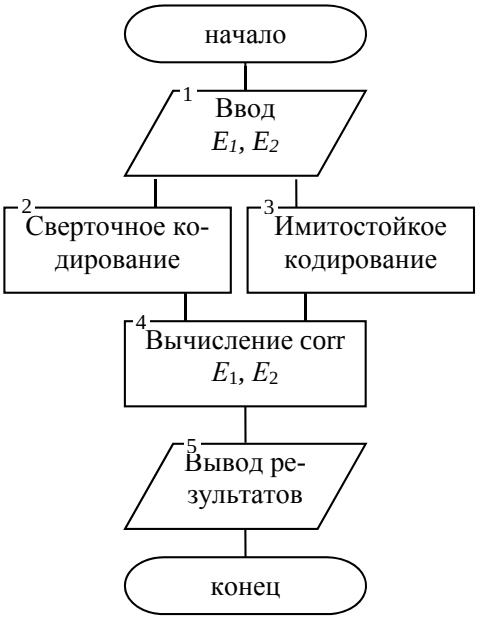

Рис. 4. Блок-схема алгоритма проведения эксперимента по оценки коэффициента корреляции криптограмм

Для определения коэффициента корреляции r криптограмм использовалось следующее выражение [8]:

$$r(E_1, E_2) = \frac{\sum_{n=1}^{N}\left(f1_n - \overline{f}1\right)\times(f2_n - \overline{f}2)}{\sqrt{\sum_{n=1}^{N}(f1_n - \overline{f}1)^2 \times \sum_{n=1}^{N}\left(f2_n - \overline{f}2\right)^2}}$$

где:

E_1 – криптограммы, полученные в результате применения имитостойкого сверточного кодирования с шифрованием информации;

E_2 – криптограммы, полученные в результате применения сверточного кодирования без шифрованием информации.

В результате получено значение коэффициента корреляции между криптограммами r=0,99, что подтверждает сформированную гипотезу, т.е. суммирование корректирующих символов с гаммой шифра не ухудшают статистических свойств сверточного кода, соответственно выигрыш от применения имитостойкого сверточного кодирования возможно оценивать известным математическим аппаратом теории кодирования.

Результаты работы программных средств подтверждают теоретические исследования по обеспечению имитостойкости информации и позволяют получить статистические данные для проведения расчета вероятности навязывания ложной информации.

Для оценки вероятности навязывания ложной информации предлагается два подхода:

1) криптографический: $P_{нав}(y') = P(\chi^{-1} y \in X)$, где χ – ключевая информация.

В данном случае вероятность навязывания ложной информации зависит от вероятности подбора (раскрытия) ключа имитопреобразования

2) кодовый: $P_{нав}(y') = f(\frac{D_{инф}}{D_{код}})$,

где:

$D_{инф}$ – информационная избыточность;

$D_{код}$ – кодовая избыточность.

В данном случае рассматривается зависимость вероятности навязывания ложной информации от ее избыточности. Частный случай для безизбыточной информации, когда $D_{инф}$=1:

$P_{нав}(y') = \frac{1}{2^n}$, где n – длина кодовой комбинации.

Применение алгоритма имитостойкого сверточного кодирования уменьшает вероятность навязывания ложной информации за счет увеличения кодовой избыточности сообщения.

Таким образом, предложена методики оценки эффективности функционирования АПД, отличающеяся от известных дополнительно введенными исходными данными и расчетными соотношениями, учитывающими имитационные помехи противника и позволяющей выполнять эту оценку на основе выходных данных, полученных в результате имитационного моделирования с применением разработанного комплекса программных средств. Ввиду простоты, корректности и адекватности имитационной модели обработки информации и допустимой точности получаемых результатов разработанная методика может использоваться при оценке разрабатываемой АПД.

Литература

1. Изделие ПД-401. Руководство по эксплуатации. Руководство оператора. РУ2.148.202 РЭ2.

2. Орощук И.М. Оценка эффективности имитоатаки радиоканала с замираниями при использовании частотной манипуляции // Известия ЮФУ. Технические науки. 2003. № 4 (33). С. 298–303.

3. Овчаренко М.В. Принципы повышения помехозащищенности аппаратуры передачи данных в автоматизированных системах управления [Текст] // Теоретические и прикладные вопросы науки и образования: сборник научных трудов по материалам Международной научно-практической конференции 31 января 2015 г.: в 16 частях. Часть 11. М-во обр. и науки РФ. Тамбов: Изд-во ТРОО «Бизнес-Наука-Общество, 2015. С. 96, 97.

4. Овчаренко М.В. Современный анализ проблемы обеспечения имитостойкости систем передачи информации / М.В. Овчаренко, А.В. Винокуров, Ю.А. Яблоновский // Информационная безопасность - актуальная проблема современности. Совершенствование образовательных технологий подготовки специалистов в области информационной безопасности: Сборник трудов VIII-IX Всероссийских научно-технических школ-семинаров. Краснодар: ФВАС. 2014. С. 169–172.

5. Свидетельство № 2014660952, дата государственной регистрации в Реестре программ для ЭВМ 20 октября 2014 г. Имитостойкое сверточное кодирование / А.В. Винокуров, М.В. Овчаренко.

6. Меньков А.В. Теоретические основы автоматизированного управления. Учебник для вузов. М.: Издательство Оникс, 2005. 640 с.: ил.

7. Архангельский А.Я. Программирование в Delphi 7 [Текст] / А.Я. Архангельский. М. : ООО «Бином-Пресс», 2005. 1152 с.

8. Теория вероятностей и математическая статистика: учебник для студ. учреждений высш. проф. образования / В.С. Мхитарян, В.Ф. Шишов, А.Ю. Козлов. М. : Издательский центр «Академия». 2012. 416 с.

METHODS EVALUATING THE PERFORMANCE OF DATA TRANSMISSION EQUIPMENT

Ovcharenko Michael Vyacheslavovich,
Rostov-on-Don, Russian, prepod84@mail.ru

Abstract: The article examines the stages of methodology for assessing the efficiency of data transmission equipment (DTE) On the basis of the functioning of the DTE in the conditions of electronic warfare is defined by its low imitoprotection to the imposition of false information. The method of evaluating the effectiveness of the DTE, on the algorithms implemented imitoprotection convolution coding. As a result of simulation obtained new scientific results to assess the benefits from the use of algorithms imitoprotection encoding parameters: probability of correct reception and the possibility of imposing false information. Practical orientation is the ability to use software system designed to evaluate the efficacy of both existing and future DTE in its inception.

Keywords: data transmission equipment, imitoprotection, simulation, methodology.

References

1. The product PD-401. Manual. Operator's Manual. RU2.148.202 RE2.
2. Oroschuk, I.M. Evaluating the effectiveness of imitoattack radio channel fading by using frequency-shift keying // Proceedings of SFU. Technical science. Number 4, 2003. (33). pp. 298-303.
3. Ovcharenko, M.V. Principles increasing immunity of data in automated control systems / Theoretical and applied problems of science and education: collection of scientific papers on the materials of the International scientific and practical conference on January 31 2015, .: 16 parts. 11. The Ministry of Education and Science. Tambov, publishing house TROO «Business-Science Society», 2015. pp. 96, 97.
4. Ovcharenko, M.V. Modern analysis of the problem of providing imitoprotection information transfer systems / M.V. Ovcharenko, A.V. Vinokurov, Y.A. Yablonovsky // Information security - actual problem of our time. Improving the educational technology training in the field of information security: Proceedings of the VIII-IX All-Russian scientific-technical schools seminars. Krasnodar FVAS, 2014. pp. 169-172.
5. The certificate number 2014660952, date of state registration in the Register of Computer Programs October 20, 2014. Imitoprotection convolution coding / A.V. Vinokurov, M.V. Ovcharenko.
6. Men'kov, A.V. Theoretical Foundations of automated control / A.V. Men'kov, V.A. Ostreykovsky. - The textbook for high schools. M .: Publishing Onyx, 2005. 640 p.
7. Archangelscay, AJ Programming in Delphi 7 / A.Y. Archangelscay. - Moscow: OOO «Bean-Press», 2005. - 1152 p.
8. Probability theory and mathematical statistics: the textbook for students. institutions of higher. prof. Education / V.S. Mkhitaryan, V.F. Shishov, A.Y. Kozlov. - Moscow: Publishing Center «Academy», 2012. - 416 p.

Information about author: Ovcharenko M.V., chief - assistant chief of staff of the m/u 12628.