НАУЧНЫЕ СООБЩЕНИЯ

И.В. Лазарев

СИНТЕЗ УСТРОЙСТВ КЛАССИФИКАЦИИ ОБЪЕКТОВ В УСЛОВИЯХ РАДИОЭЛЕКТРОННОГО КОНФЛИКТА

SYNTHESIS OF DEVICES OF CLASSIFICATION OF OBJECTS IN THE CONDITIONS OF CONFLICT RADIOELECTRONIC

На основе анализа современного состояния радиоэлектронной борьбы и принципов построения радиоэлектронных систем определены особенности, присущие различным этапам синтеза устройств классификации. Унифицирован процесс синтеза устройств классификации на основе структурно-функциональной архитектуры, позволяющий осуществлять обоснованный выбор варианта построения устройства классификации.

On the basis of the analysis of a current state of radio-electronic fight and the principles of creation of radio-electronic systems the features inherent in various stages of synthesis of devices of classification are defined. Process of synthesis of devices of classification on the basis of the structurally functional architecture, allowing to carry out a reasonable choice of option of creation of the device of classification is unified.

В современных условиях на специальные радиотехнические средства (РТС), используемые, например, для мониторинга воздушного пространства, возлагают задачи: обнаружения, измерения координат, определения параметров движения, а также задачи распознавания или идентификации (определения класса или типа) объекта.

В последние годы в активной локации широко используются широкополосные сигналы, которые обеспечивают большую информативность, в частности, вследствие обработки дальностных радиолокационных портретов (ДРЛП), представляющих собой видеоимпульсы сложной формы, структура которых зависит от геометрии летательного объекта. Использование ДРЛП позволяет решить задачу классификации объектов, выделив в них в простейшем случае следующие три класса: малоразмерные, среднеразмерные и крупноразмерные [1].

Однако большинство алгоритмов классификации получены для случая простой фоновой обстановки, характеризующейся наличием лишь широкополосного флуктуационного шума. При этом для решения задачи классификации объектов необходимо задавать множество [2], элементы которого характеризуют как условия решения задачи, так и накладываемые ограничения, включая технические:

$$\{F\}=(A,X,R,Y,J_p). \quad (1)$$

Здесь: A — пространство классов;

X — пространство признаков;

R — пространство решающих правил;

Y — пространство устройств классификации объектов;

J_p — вектор, включающий в себя показатели, характеризующие эффективность, финансовые и временные затраты [3].

Вместе с тем в будущих конфликтах противоборствующая сторона (вероятный противник) будет стремиться использовать различные виды помех, в частности, шумовые и импульсные, направленные на существенное усложнение фоновой обстановки.

В условиях сложной фоновой обстановки необходимо дополнительно ввести в рассмотрение пространство помех N. Тогда множество (1) перепишется в виде

$$\{F\}=(A,X,R,Y,N,J_p). \quad (2)$$

В выражении (2) могут быть заданы все или отсутствовать один из первых трех элементов, что и определяет тип задачи распознавания объектов, а конкретные подходы к заданию элементов **A, X, R, N** определяют модель процесса распознавания объектов. Следовательно, возможно несколько подходов к вариантам типовых задач распознавания объектов.

Реализация процедуры классификации объектов (распознавание сигналов) предусматривает два этапа: узкополосный и широкополосный, а процесс наблюдаемых данных может быть описан одной из следующих аддитивных моделей:

$$x_1(t) = n(t) + \gamma_0 S_y(t);$$

$$x_2(t) = n(t) + \gamma_1 N(t) + \gamma_2 S(t), \quad (3)$$

где $n(t)$ — белый гауссов шум;

$N(t)$ — преднамеренная помеха;

$S_y(t)$, $S(t)$ — полезные сигналы при узкополосном и широкополосном зондировании;

γ_0, γ_1, γ_2 — коэффициенты, принимающие значения 0 и (или) 1.

При этом на этапе узкополосной обработки входная реализация — это $x_1(t)$, а на широкополосном этапе — $x_2(t)$. В узкополосном тракте решается задача обнаружения сигнала и измерения некоторых (траекторных) параметров. Если в узкополосном тракте вынесено решение об отсутствии сигнала, то в широкополосном тракте решается задача различения преднамеренных помех. Далее, при обнаружении сигнала в узкополосном тракте, в широкополосном тракте решается задача распознавания сигналов либо при наличии, либо при отсутствии преднамеренной помехи (в зависимости от того, какое решение выработал тракт различения преднамеренных помех).

Из вышеизложенного следует, что распознающая система должна соответствовать следующим требованиям:

в узкополосном тракте регистрировать факт обнаружения сигнальной смеси и выдавать результат в широкополосный тракт;

в тракте траекторного измерения осуществлять оценки параметров (например, ракурса) объекта и выдавать их в широкополосный тракт;

в широкополосном тракте иметь тракт сигнального распознавания, осуществляющего решение задачи классификации объектов в условиях простой фоновой обстановки (в выражении (3) коэффициент $\gamma_1 = 0$);

автоматически обрабатывать преднамеренные помехи в тракте различения помехи и выдавать результаты анализа (различения) в тракты сигнального распознавания в условиях простой и сложной фоновой обстановки;

затрачивать минимальное время (отвечать реальному масштабу времени) при обработке информации и принятии решения о классе объекта.

Таким образом, структурную схему распознающей системы (системы классификации) можно представить в виде, изображенном на рис. 1.

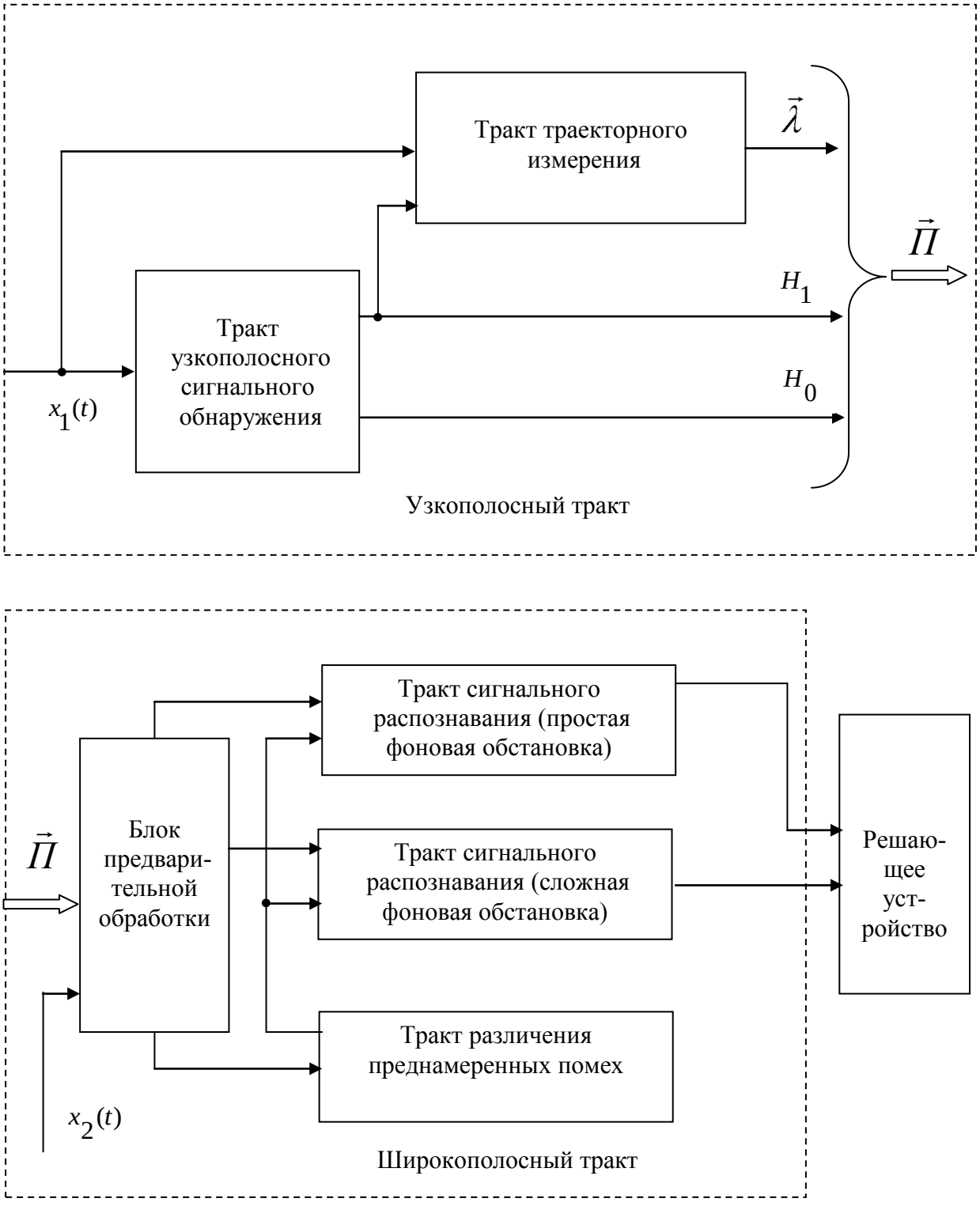

Рис. 1. Структурная схема распознающей системы в условиях радиоэлектронного конфликта

На рис. 1 пунктиром выделены узкополосный и широкополосный тракты. В узкополосном тракте при поступлении реализации $x_1(t)$ (выражение (3)) решаются задачи сигнального обнаружения (выносится решение либо в пользу гипотезы H_1 — сигнал присутствует, либо в пользу гипотезы H_0 — сигнал отсутствует в реализации наблюдаемых данных) и, если выносится решение о наличии сигнала, то осуществляется измерение вектора параметров $\vec{\lambda}$ сигнала. Полученный вектор $\vec{\Pi} = \left\| \vec{\lambda}, H_i \right\|$, $i = 0$ или 1, поступает на вход блока предварительной обработки широкополосного тракта.

В широкополосном тракте на вход этого же блока поступает реализация $x_2(t)$ (выражение (3)). Далее в тракте различения преднамеренных помех решается задача различения помех различного типа. В зависимости от ее решения, задача классификации объектов решается в одном из трактов сигнального распознавания (в условиях простой или сложной фоновой обстановки). Наконец, в решающем устройстве выносится решение о наличии сигнала определенного класса на входе распознающей системы.

Анализ рис. 1 свидетельствует о том, что система распознавания в условиях радиоэлектронного конфликта представляет собой иерархическую структуру, в которой вероятность выполнения задачи классификации объектов, с учетом [4], может быть представлена в виде

$$P = \prod_{i=1}^{m} (1 - P_i). \qquad (4)$$

Здесь P_i — вероятность невыполнения задач по своему функциональному назначению, $i = \overline{1,3}$.

Данные обстоятельства требуют решения ряда задач, связанных с использованием алгоритмов обработки информации, адаптивных к уровню не только флуктуационных шумов, но и преднамеренных помех, и применения решающих правил, обеспечивающих требуемую эффективность распознавания объектов в реальном масштабе времени в условиях радиоэлектронного конфликта.

Вышеуказанные особенности обусловливают существенные требования к устройствам классификации как на этапе обработки информации, так и на этапе выдачи результатов распознавания в систему управления. При этом процесс синтеза устройств классификации может осуществляться на основе структурно-функциональной архитектуры и включает ряд этапов (рис. 2).

На блок-схеме рис. 2 приняты обозначения: ФО — фоновая обстановка, К — выход (завершение процедуры) из алгоритма.

Анализ блок-схемы рис. 2 свидетельствует о том, что процесс синтеза структуры устройства классификации носит итеративный характер и может быть разбит на несколько последовательных шагов:

1. Осуществляется формулировка задачи. Вводится в рассмотрение пространство классов **A**.

2. На основе анализа возможных вариантов решения задачи классификации объектов, исходя из сигнальной информации выбирается математических метод, наиболее адекватный поставленной задаче.

3. Анализируются условия классификации объектов на фоне простой и сложной обстановки, выбирается соответствующий рабочий словарь признаков.

4. С учетом возможных типов преднамеренных помех синтезируется алгоритм их различения.

5. На основе рабочего словаря признаков синтезируется алгоритм распознавания классов объектов и оценивается суммарная сложность его организации.

6. В соответствии с разработанным алгоритмом классификации производится выбор структуры устройства классификации объектов.

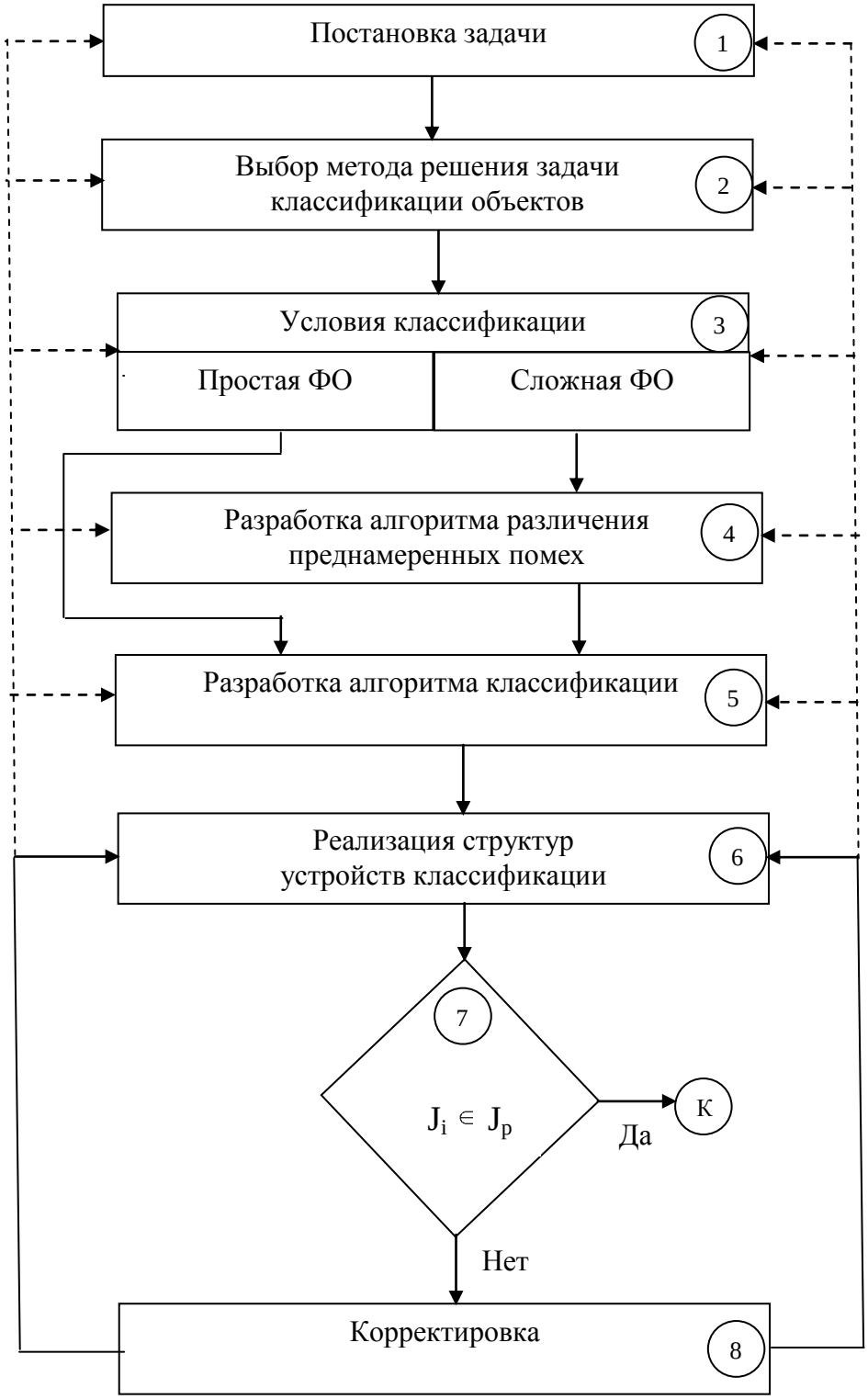

Рис. 2. Блок-схема алгоритма синтеза устройств классификации тракта сигнального распознавания в условиях радиоэлектронного конфликта

7. Если показатели $\mathbf{J_i}$, характеризующие эффективность, финансовые и временные затраты синтезированного устройства, удовлетворяют заданным требованиям, т.е. условие блока (7) выполнено, то процедура завершается (выход К).

В случае невыполнения условия блока (7) необходимо осуществить корректировку (блок 8), которая заключается либо в совершенствовании вариантов устройств классификации, например в соответствии с рекомендациями [2], либо в корректировке алгоритма классификации или метода распознавания, а в исключительных случаях — постановку задачи синтеза, а также исходных данных, тактико-технических требований.

Применение предложенного подхода при синтезе устройств классификации объектов позволит разработчикам аппаратуры осуществлять обоснованный выбор варианта построения системы распознавания в условиях радиоэлектронного конфликта.

ЛИТЕРАТУРА

1. Радиоэлектронные системы: основы построения и теория. Справочник / Я.Д. Ширман [и др.]; под ред. Я.Д. Ширмана. — М.: ЗАО «Маквис», 2007.

2. Лазарев И.В. Постановка задачи оптимизации распознающей системы в условиях структурно-функциональной архитектуры // Вестник Воронежского института МВД России. — 2011. — № 3 — С. 120—127.

3. Булгаков О.М., Лазарев И.В. Метод синтеза структур микропроцессорных устройств классификации воздушных объектов по критерию «эффективность — интегрированные затраты» в условиях параметрической априорной неопределенности // Вестник Воронежского института МВД России. — 2010. — № 2 — С. 109—114.

4. Вентцель Е.С. Исследование операций. — М.: Сов. радио, 1972.

СВЕДЕНИЯ ОБ АВТОРЕ

Лазарев Иван Владимирович. Начальник кафедры радиотехники. Кандидат технических наук, доцент.

Воронежский институт МВД России.

E-mail: vorhmscl @ comch.ru

Россия, 394065, г. Воронеж, проспект Патриотов, 53. Тел.(473)2623-279.

Lazarev Ivan Vladimirovich. The chief of the radio engineering chair. Candidate of technical sciences, assistant professor.

Voronezh Institute of the Ministry of the Interior of Russia.

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53. Tel. (473) 2623-279.

Ключевые слова: преднамеренные помехи; радиоэлектронный конфликт; устройства классификации объектов.

Key words: deliberate hindrances; radio-electronic conflict; devices of classification of objects.

УДК 621.396

Д.А. Жайворонок, О.С. Сластникова

ПОВЫШЕНИЕ БЫСТРОДЕЙСТВИЯ ОДНОКОЛЬЦЕВОГО СИНТЕЗАТОРА ЧАСТОТ

THE SPEED RISE OF THE ONE-RING FREQUENCY SYNTHESIZER

Рассмотрен метод повышения быстродействия синтезатора частот на основе кольца импульсно-фазовой автоподстройки частоты. Описана структурная схема синтезатора и проверен анализ его работы.

The speed rise of the one-ring frequency synthesizer method on basis of the frequency impulse-phase self-tuning is considered.The synthesizer structured diagram is described, procedure analysis is produced.

Широко известен синтезатор частот (СЧ), построенный по однокольцевой схеме импульсно-фазовой автоподстройки частоты (ИФАПЧ), структурная схема которого изображена на рис. 1.

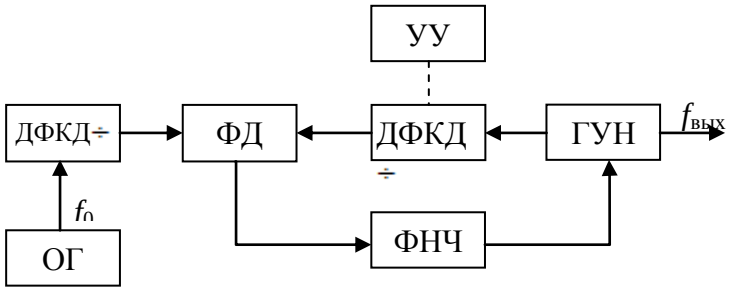

Рис. 1. Структурная схема однокольцевого синтезатора частот с ИФАПЧ

Синтезатор частот содержит генератор управляемый напряжением (ГУН), делитель с переменным коэффициентом деления (ДПКД) и с устройством управления (УУ), фазовый детектор (ФД) и фильтр нижних частот (ФНЧ). К другому входу ФД через делитель частоты с фиксированным коэффициентом деления (ДФКД) подключен выход высокостабильного опорного кварцевого генератора (ОГ).

В режиме синхронизма входная частота синтезатора определяется по формуле

$f_{вых} = f_0 N/R$,

где f_0 — частота опорного генератора;

N — коэффициент деления ДПКД;

R — коэффициент деления ДФКД.

Такой синтезатор частот характеризуется простой реализацией, высокой надежностью и технологичностью, обладает возможностью сформировать необходимое число частот, но имеет существенный недостаток, который вытекает из принципа работы такого СЧ. Этот недостаток состоит в том, что невозможно выбирать частоту сравнения $f_{ср} = f_0/R$ выше заданного шага сетки частот. Следовательно, при мелком шаге сетки частот и импульсном характере частоты сравнение быстродействия синтезатора значительно снижается.

Повысить быстродействие можно, применив следующее техническое решение. В синтезатор частот, содержащий последовательно соединенные ГУН, ДПКД с устрой-

ством управления, последовательно вводятся ОГ и ДФКД, а также первый ФНЧ, первый и второе формирующее устройство (ФУ), второй ФНЧ первый и второй фазовращатели на π/2, первый и второй перемножители сигналов (ПС) и вычитатель (В).

На рис. 2 приведена структурная электрическая схема предлагаемого синтезатора частот.

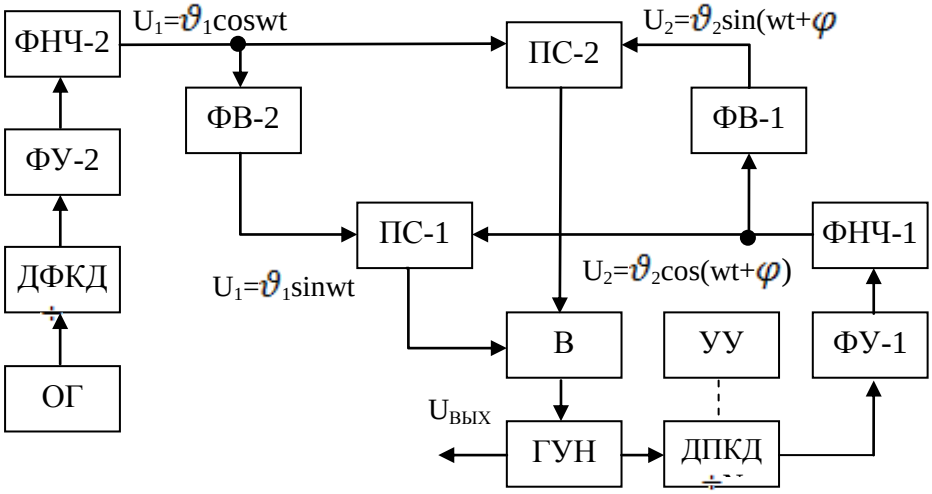

Рис. 2. Структурная схема однокольцевого синтезатора частот с квадратурным преобразованием сигналов

Синтезатор частот работает следующим образом. Импульсы с частотой сравнения с ДФКД с помощью ФУ-2 преобразуются в импульсы по форме «меандр» и поступают на вход ФНЧ-2, который их преобразует в гармонический сигнал $U_1=\vartheta_1\cos wt$. Этот сигнал поступает на первый вход перемножителя сигналов ПС-2 и через фазовращатель на π/2 ФВ-2 на второй вход перемножителя ПС-1 в виде сигнала сигнал $U_1=\vartheta_1\sin wt$ (т.е. произошло квадратурное расщепление опорного сигнала). В режиме синхронизма импульсы с ДПКД с помощью ФУ-1 преобразуются в импульсы, близкие по форме к «меандру» и поступают на вход ФНЧ-1, который преобразует их в гармонический сигнал $U_2=\vartheta_2\cos(wt+\varphi)$. Этот сигнал поступает на первый вход перемножителя ПС-1 и через фазовращатель на π/2 ФВ-1 на второй вход второго перемножителя в виде $U_2=\vartheta_2\sin(wt+\varphi)$. После перемножения на выходе второго перемножителя ПС-2 имеется

$$U_{ВЫХ1}=K_{П1}\vartheta_1\,\vartheta_2\sin(wt+\varphi)\cos wt\,, \quad (1)$$

где $K_{П1}$ — коэффициент преобразования перемножителя ПС-2, имеющий размерность Вольт $^{-1}$.

На выходе первого перемножителя ПС-1 получится сигнал

$$U_{ВЫХ2}=K_{П2}\vartheta_1\,\vartheta_2\cos(wt+\varphi)\sin wt. \quad (2)$$

Считая $K_{П1}= K_{П2}= K_П$, в результате алгебраического сложения (1) и (2) получаем на выходе вычитателя (В)

$$U_{ВЫХВ}= K_{П1}\vartheta_1\,\vartheta_2\sin(wt+\varphi)\cos wt - K_{П2}\vartheta_1\,\vartheta_2\cos(wt+\varphi)\sin wt= K_П\,\vartheta_1\,\vartheta_2\sin\varphi. \quad (3)$$

Напряжение сигнала $U_{ВЫХВ}$ поступает на управляющий вход ГУН и подстраивает его частоту под опорный сигнал с точностью до фазы φ.

Поскольку напряжение на выходе вычитателя соответствует только разности фаз φ и свободно от побочных колебаний, то фильтр на выходе вычитателя в цепи управления ГУН не нужен.

В переходном режиме при переключении с одной частоты на другую путем изменения коэффициента деления ДПКД N разность фаз изменится и на выходе ФНЧ-1 получится сигнал $U_2= \vartheta_2 \cos(wt+\Delta wt+wt+\varphi)$. При этом новое управляющее напряжение с выхода вычитателя $U_{ВЫХВ}= K_{П1}\vartheta_1 \vartheta_2 \sin(wt+\varphi)$ соответствует новому значению частоты ГУН.

Выигрыш в быстродействии по сравнению с прототипом здесь заключается в отсутствии ФНЧ на выходе вычитателя в цепи управления ГУН в синтезаторе-прототипе.

Например, пусть будет частота сравнения (и соответственно шаг сетки частот) $f_{ср}$=10кГц. При этом частота среза первого и второго ФНЧ немного больше 10кГц, чтобы пропустить только первую гармонику и получить синусоидальный сигнал. В то же время ФНЧ на выходе ФД в СЧ-прототипе $f_{ср}$=10кГц должен быть такой, чтобы частота среза его была, по крайней мере, меньше 100Гц (т.е. на два порядка меньше) для получения необходимого подавления помех от частоты сравнения.

Иначе говоря, ФНЧ в цепи управления ГУН в СЧ-прототипе должен быть примерно в 100 раз более инерционный, чем ФНЧ в цепи обратной связи предложенного синтезатора, т.е. полоса пропускания кольца ФАПЧ в предложенном синтезаторе намного больше. Отсюда и выигрыш по быстродействию будет соответствующий.

Подстройка фазы в предложенном СЧ происходит непрерывно, так как сравниваются аналоговые сигналы, а не импульсные, как в СЧ-прототипе, что также повышает быстродействие.

ЛИТЕРАТУРА

1. Четкин О.В., Хохлов Н.С. Частотные характеристики тандемных цифровых синтезаторов частот с угловой модуляцией управляемого и опорного генераторов // Вестник Воронежского государственного технического университета. — 2009. — Т. 5. — №4. — С. 72—75.

2. Манасеевич В. Синтезаторы частот (Теория и проектирование): пер. с англ. / под ред. А.С. Галина. — М.: Связь, 1979. — 384 с.

3. Шахгильдян В.В., Ляховкин А.А. Системы фазовой автоподстройки частоты. — М.: Связь, 1972. — 448 с.

СВЕДЕНИЯ ОБ АВТОРАХ

Жайворонок Денис Александрович. Доцент кафедры телекоммуникационных систем. Кандидат технических наук, доцент.

Воронежский институт МВД России.

Россия, 394065, г. Воронеж, проспект Патриотов, 53. Тел. (473) 2476-485.

Сластникова Ольга Сергеевна. Начальник отделения Центра информационных технологий, связи и защиты информации УМВД по Ханты-Мансийскому АО — Югре.

Россия, 628000, г. Ханты-Мансийск, ул. Ленина, 55. Тел. (4346) 739-8810.

Zhayvoronok Denis Alexandrovich. Assistant professor of Telecommunication Systems chair. Candidate of technical sciences, assistant professor.

Voronezh Institute of the Ministry of the Interior of Russia.

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53. Tel. (473) 2476-485.

Slastnikova Olga Sergeevna. The Head of division of Centre of Informatic Technologies, Communications and Information Protection of the Department of Internal Affairs on Khunts-Mansies autonomous region — Jugra.

Work address: Russia, 628000, Khanty-Mansiysk, Lenin Str.,55. Tel. (4346) 739-8810.

Ключевые слова: синтезатор частот; импульсно-фазовая автоподстройка частоты; сетка частот; быстродействие.

Key words: synthesizer of frequencies; pulse and phase auto-adjust of frequency; grid of frequencies; speed.

УДК 621.396.42

И.Г. Дровникова, А.А. Никитин

ОСОБЕННОСТИ ИСПОЛЬЗОВАНИЯ СТАНДАРТОВ СЕРИИ ISO 9000 ДЛЯ ОБЕСПЕЧЕНИЯ КАЧЕСТВА ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ ПАРИРОВАНИЯ НЕГАТИВНЫХ ИНФОРМАЦИОННЫХ ВОЗДЕЙСТВИЙ

FEATURES OF USE OF STANDARDS OF THE ISO 9000 SERIES FOR ENSURING QUALITY FUNCTCION OF SYSTEM PARRYINGS OF NEGATIVE INFORMATION IMPACTS

Проведен анализ существующего порядка разработки системы парирования негативных информационных воздействий в автоматизированных системах (АС). Исходя из требований стандартов серии ISO 9000, предложена система показателей дополнительных требований к системе парирования негативных информационных воздействий, которые необходимо учитывать на ранних стадиях проектирования данных систем.

The analysis of an existing order of development of the system of parrying of negative information impacts in the automated systems is carried out. Proceeding from requirements of standards of the ISO 9000 series, the system of indicators of additional requirements to system of parrying of negative information impacts which are necessary for considering at early design stages of these systems is offered.

В настоящее время система парирования негативных информационных воздействий (СПНИВ) является подсистемой системы защиты информации (ЗИ) в АС и представляет собой отдельный программно-технический комплекс (ПТК), который нейтрализует различные дестабилизирующие воздействия, включая и угрозы несанкционированного доступа (НСД) нарушителя, связанные с нарушением конфиденциальности, доступности и целостности информации в АС. При разработке таких ПТК обоснованием требований к этим системам выступают руководящие документы [1—3].

Особенностью данных документов является использование функционального подхода с точки зрения задания требований к СПНИВ. Требования к остальным характеристикам, обычно используемым при проектировании для формального взаимодействия разработчика и заказчика СПНИВ, в этих документах не содержатся. Поэтому в начальный период проектирования СПНИВ использовать руководящие документы достаточно сложно.

На основе обобщения зарубежного опыта по созданию качественного программного обеспечения сформировалась система управления качеством программных систем (ПС). Базовые положения этой системы легли в основу стандартов ISO серии 9000. Основным здесь является утвержденный в 1991 г. международный стандарт ISO 9126:1991 «Информационная технология. Оценка программного продукта. Характеристики качества и руководство по их применению» [4]. Данным стандартом рекомендуется 6 основных характеристик качества ПС, каждая из которых детализируется несколькими субхарактеристиками (всего 21). В стандарте предусмотрены следующие

характеристики качества ПС: функциональность, надежность, удобство использования, эффективность, сопровождаемость, мобильность.

Требования к набору функциональных характеристик СПНИВ полностью определяются нормативными документами [1—3] в соответствии с ее классом защищенности (профилем защиты, используемым при разработке задания по безопасности). Поэтому наличие сертификата свидетельствует о реализации в ПС всех требуемых функций, следовательно, данную характеристику для СПНИВ использовать нецелесообразно.

Для выбора показателя количественной оценки надежности СПНИВ рассмотрим некоторые особенности функционирования данных систем. Характерной особенностью СПНИВ как сложной ПС является возможность автоматизированного восстановления работоспособности программными методами [5], имеющими достаточно малое время и позволяющими отказы ПС преобразовать в сбои. Другой важной особенностью для обоснования показателя, характеризующего надежность СПНИВ, является диалоговый режим ее работы. При этом в качестве субъекта доступа в большинстве случаев выступает человек. С учетом этого, и приняв независимыми процессы отказов, восстановлений и оперативного контроля, в качестве интегрального показателя, характеризующего надежность СПНИВ, целесообразно выбрать коэффициент готовности ($K_г$).

Применительно к защищенным АС можно выделить две основные категории пользователей. Первая категория — использующие АС при работе с конфиденциальной информацией. Применение СПНИВ этой категорией пользователей ограничивается введением своей идентификационной и аутентификационной информации. Остальные механизмы безопасности информационных технологий (управление доступом, контроль целостности, учет и регистрация событий в системе) осуществляются без участия пользователя. Доступность, понятность и полнота описания взаимодействия пользователя данной категории с СПНИВ гарантируется наличием сертификата по требованиям ЗИ от НСД. В руководящих документах [1—3] требования к эксплуатационной документации изложены достаточно полно.

Вторая категория пользователей — администраторы СПНИВ, часто именуемые офицерами обеспечения безопасности информационных технологий. Наличие, понятность и полнота документации администратора СПНИВ также гарантируются сертификатом по требованиям ЗИ от НСД.

Основными функциями администратора СПНИВ являются: установка, проверка и настройка СПНИВ, просмотр журнала регистрации и обработка событий НСД, блокировка и разблокировка ЭВМ, тестирование, контроль и управление работой СПНИВ. Характеризовать удобство выполнения администратором СПНИВ своих функций целесообразно лингвистическим показателем «Удобство эксплуатации и обслуживания администратором».

При проведении анализа временной эффективности и ресурсоемкости необходимо рассмотреть два возможных режима работы АС: диалоговый и режим реального времени. Отличительной особенностью первого режима работы является ожидание АС команд от пользователя и выдача ему результатов расчетов. Особенность второго режима заключается в наличии случайного непрерывного потока заданий на исполнение в течение определенного времени, которое нельзя превышать.

Обнаружение СПНИВ в составе программного обеспечения АС отнимает для выполнения своих процедур часть вычислительного ресурса, и в тоже время нагрузка на вычислительную систему, вызванная выполнением функций СПНИВ, связана с интенсивно-

стью решения своих задач по прямому назначению. Поэтому затраты ресурсов АС на выполнение процедур СПНИВ удобно характеризовать относительной величиной.

Для первого режима работы целесообразно применять безразмерный показатель относительного увеличения среднего времени решения основных функциональных задач Δ_T, который имеет вид:

$$\Delta_T = \frac{T_{срСПНИВ} - T_{ср}}{T_{ср}} \text{ x100\%}, \quad (1)$$

где $T_{ср}$ — среднее время решения основных вычислительных задач АС без СПНИВ, выраженное в секундах (по системе СИ); $T_{срСПНИВ}$ — среднее время решения основных вычислительных задач АС при наличии СПНИВ, выраженное в секундах (по системе СИ).

Для второго режима работы используется выраженный в процентах показатель относительного увеличения загрузки процессора АС Δ_p, измеряемой специализированным программным комплексом:

$$\Delta_\rho = \frac{\rho - \rho_{СПНИВ}}{\rho} \text{ x100\%}, \quad (2)$$

где ρ — загрузка процессора АС без СПНИВ, выраженная в мегабайтах; $\rho_{СПНИВ}$ — загрузка процессора АС при наличии СПНИВ, выраженная в мегабайтах.

Таким образом, в данной статье проведен анализ различных нормативных документов, связанных с проблемой обеспечения ИБ в существующих АС, и порядка разработки СПНИВ в этих системах. Исходя из требований стандартов серии ISO 9000, предложена система показателей качества функционирования СПНИВ, позволяющая проводить интегральную оценку эффективности этих систем при разработке АС в защищенном исполнении.

ЛИТЕРАТУРА

1. Гостехкомиссия России. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. — М.: Военное издательство, 1992.

2. Гостехкомиссия России. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. — М.: Военное издательство, 1992.

3. ГОСТ Р ИСО/МЭК 15408 — 2002. Информационная технология. Методы и средства обеспечения безопасности информационных технологий.

4. Сборник действующих международных стандартов ИСО серии 9000. Т.1,2,3. — М.: ВНИИКИ, 1998.

5. Липаев В.В. Качество программного обеспечения. — М.: Финансы и статистика, 1983. — 250 с.

СВЕДЕНИЯ ОБ АВТОРАХ

Дровникова Ирина Григорьевна. Профессор кафедры автоматизированных информационных систем ОВД. Доктор технических наук, доцент.
Воронежский институт МВД России.
E-mail: idrovnikova@mail.ru
Россия, 394065, г. Воронеж, проспект Патриотов, 53. Тел. (473)262-32-78.

Никитин Александр Александрович. Инженер.
В/Ч 28683.
E-mail: sansanych@bk.ru
Россия, 394042, г. Воронеж, ул. Минская, 2. Тел. (473)223-27-40.

Drovnikova Irina Grigoryevna. Professor of the chair of Automatic Information Systems. Doctor of technical sciences, assistant professor.
Voronezh Institute of the Ministry of the Interior of Russia.
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53. Tel. (473)262-32-78.

Nikitin Alexander Alexandrovich. Engineer.
Military division N 28683.
Work address: Russia, 394042, Voronezh, Minskaya Str., 2. Tel. (473)223-27-40.

Ключевые слова: система парирования негативных информационных воздействий; автоматизированная система; информационная безопасность.

Key words: system of parrying of negative information impacts; automated system; information security.

УДК 621.3

ИЗДАНИЯ ВОРОНЕЖСКОГО ИНСТИТУТА МВД РОССИИ

Овсянников И.В.
Документальные проверки и ревизии как квазипроцессуальный феномен: монография / И.В. Овсянников. — Воронеж: Воронежский институт МВД России, 2013. — 132 с.

Проводится сравнительный анализ данного института и института судебной экспертизы. Исследуется проблемный вопрос о доказательственном значении акта документальной проверки, ревизии. В криминалистическом аспекте вскрываются негативные последствия производства документальных проверок, ревизий на стадии возбуждения уголовных дел о преступлениях экономической направленности.
Предназначена для следователей, дознавателей, прокуроров, адвокатов, судей, а также для научных работников, преподавателей, адъюнктов (аспирантов), студентов (слушателей, курсантов) юридических учебных заведений.

В.К. Джоган, А.О. Авсентьев

СПОСОБ ПРЕДСТАВЛЕНИЯ МАТЕМАТИЧЕСКИХ МОДЕЛЕЙ ДЛЯ ОЦЕНКИ ХАРАКТЕРИСТИК ПРОТИВОДЕЙСТВИЯ ПЕРЕХВАТУ РЕЧЕВОЙ ИНФОРМАЦИИ

METHOD OF PRESENTING MATHEMATICAL MODELS FOR ESTIMATING CHARACTERISTICS OF CONTRAACTION AGAINST VOICE INFORMATION INTERCEPTION

В качестве средства первичной формализации противоправных действий по перехвату речевой информации рассматривается способ представления функциональной модели такого рода действий в рамках символьного моделирования, позволяющий существенно упростить в дальнейшем переход от функционального к математическому их представлению. Рассмотрены варианты продукций последовательной и параллельной очередности реализации частных функций декомпозиции целевой предметной функции противоправных действий по перехвату речевой информации.

This paper considers as means of primary formalization of illegal actions to intercept voice information, the method of presentation of the functional model of the kind within the framework of symbolic modelling, which allows simplifying further transaction from functional to their mathematical representation. This work views productions versions of sequential and parallel sequence of realization of particular functions of decomposition of the target objective function of illegal actions in intercepting voice information.

Одним из наиболее распространенных способов первичной формализации информационных процессов является функциональное моделирование [1], нашедшее целый ряд применений в приложениях теории информационной безопасности [2]. Вместе с тем при использовании известных структурных методологий [1] в качестве средства первичной формализации исследуемых процессов возникают трудности перехода от графического функционального к строго формализованному (аналитическому или имитационному) математическому их представлению. Для устранения такого рода трудностей целесообразно представление функциональной модели в рамках аппарата символьного моделирования [3].

Представим в формате символьного моделирования многоуровневую композиционную функциональную модель противодействия утечке речевой информации продукциями вида:

$$<\varphi_1^{(l)} \,\&\, \ldots \,\&\, \varphi_j^{(l)} \,\&\, \ldots \,\&\, \varphi_J^{(l)}> = <\varphi_k^{(l+1)}, A_k^{(l+1)}, B_k^{(l+1)}, X_k^{(l+1)}, \Delta_k^{(l+1)}>, \quad (1)$$

$$<\varphi_1^{(l)} + \ldots + \varphi_j^{(l)} + \ldots + \varphi_J^{(l)}> = <\varphi_k^{(l+1)}, A_k^{(l+1)}, B_k^{(l+1)}, X_k^{(l+1)}, \Delta_k^{(l+1)}>, \quad (2)$$

где $\varphi_j^{(l)}$ — наименование j-й, $j = 1, 2, \ldots, J$ функции l-го уровня иерархии структуры функционального представления действий по защите речевой информации от утечки по техническим каналам;

&, + — символы, означающие булевы операции «и» и «или», соответственно.

$A^{(l+1)}$, $B^{(l+1)}$, $X^{(l+1)}$ — входные, управленческие и выходные потоки для функции $\varphi^{(l+1)}$, соответственно;

$\Delta^{(l+1)}$ — используемые данной функцией ресурсы (механизмы).

При этом продукция (1) будет соответствовать последовательной реализации частных функций, а продукция (2) — параллельной.

Множество функций $\{\varphi_i^{(1)}\}$, $i = 1, 2, \ldots, 10$, первого уровня композиционной структуры действий по защите речевой информации, полученное на основе анализа способов и средств защиты речевой информации от утечки по техническим каналам [4], будет составлять совокупность функций второго уровня такого рода структуры, что с учетом (1) и (2) позволяет их представить в виде:

$$<\varphi_1^{(1)} \,\&\, \varphi_2^{(1)}> = <\varphi_1^{(2)}, A_1^{(2)}, B_1^{(2)}, X_1^{(2)}, \Delta_1^{(2)}>, \quad (3)$$

где $\varphi_1^{(1)}$ — функция противодействия определению уровня сигнала;

$\varphi_2^{(1)}$ — функция противодействия определению значимости речевой информации;

$\varphi_1^{(2)}$ — функция защиты речевой информации от перехвата по прямым акустическим каналам;

$A_1^{(2)}$ — информация акустических полей;

$B_1^{(2)}$ — ущерб от нарушения информационной безопасности;

$X_1^{(2)}$ — отсутствие или наличие утечки речевой информации;

$\Delta_1^{(2)}$ — средства определения диктофонов;

$$<\varphi_3^{(1)} + \varphi_4^{(1)}> = <\varphi_2^{(2)}, A_2^{(2)}, B_2^{(2)}, X_2^{(2)}, \Delta_2^{(2)}>, \quad (4)$$

где $\varphi_3^{(1)}$ — функция противодействия установке закладочного устройства;

$\varphi_4^{(1)}$ — функция противодействия активированию закладочного устройства;

$\varphi_2^{(2)}$ — функция защиты речевой информации от съема/передачи;

$A_2^{(2)}$ — информация акустических полей;

$B_2^{(2)}$ — ущерб от нарушения информационной безопасности;

$X_2^{(2)}$ — отсутствие или наличие утечки речевой информации;

$\Delta_2^{(2)}$ — Средства контроля доступа в контролируемую зону;

$$<\varphi_5^{(1)} + \varphi_6^{(1)}> = <\varphi_3^{(2)}, A_3^{(2)}, B_3^{(2)}, X_3^{(2)}, \Delta_3^{(2)}>, \quad (5)$$

где $\varphi_5^{(1)}$ — функция противодействия съему информации с помощью направленного микрофона;

$\varphi_6^{(1)}$ — функция противодействия записи информации с помощью направленного микрофона;

$\varphi_3^{(2)}$ — функция защиты речевой информации от перехвата с помощью направленного микрофона;

$A_3^{(2)}$ — информация акустических полей;

$B_3^{(2)}$ — ущерб от нарушения информационной безопасности;

$X_3^{(2)}$ — отсутствие или наличие утечки речевой информации;

$\Delta_3^{(2)}$ — средства защиты информации от перехвата с помощью направленного микрофона;

$$<\varphi_7^{(1)} + \varphi_8^{(1)}> = <\varphi_4^{(2)}, A_4^{(2)}, B_4^{(2)}, X_4^{(2)}, \Delta_4^{(2)}>, \quad (6)$$

где $\varphi_7^{(1)}$ — функция противодействия определению места установки лазерной акустической системы;

$\varphi_8^{(1)}$ — функция противодействия выбору отражающей конструкции;

$\varphi_4^{(2)}$ — функция защиты речевой информации от съема с помощью лазерной акустической системы;

$A_4^{(2)}$ — информация акустических полей;

$B_4^{(2)}$ — ущерб от нарушения информационной безопасности;

$X_4^{(2)}$ — отсутствие или наличие утечки речевой информации;

$\Delta_4^{(2)}$ — средства наблюдения за прилегающей к контролируемой зоне территорией;

$$<\varphi_9^{(1)} + \varphi_{10}^{(1)}> = <\varphi_5^{(2)}, A_5^{(2)}, B_5^{(2)}, X_5^{(2)}, \Delta_5^{(2)}>, \quad (7)$$

где $\varphi_9^{(1)}$ — функция противодействия определению способа облучения;

$\varphi_{10}^{(1)}$ — функция противодействия определению вида модулятора;

$\varphi_5^{(2)}$ — функция защиты речевой информации от съема за счет ВЧ навязывания;

$A_5^{(2)}$ — информация акустических полей;

$B_5^{(2)}$ — ущерб от нарушения информационной безопасности;

$X_5^{(2)}$ — отсутствие или наличие утечки речевой информации;

$\Delta_5^{(2)}$ — средства защиты информации от утечки за счет ВЧ навязывания.

Множество функций $\{\varphi_m^{(2)}\}$, m = 1, 2, …, 5, второго уровня композиционной структуры действий по защите информации составляет совокупность функций третьего уровня такого рода структуры:

$$<\varphi_1^{(2)} \,\&\, \varphi_2^{(2)})> = <\varphi_1^{(3)}, A_1^{(3)}, B_1^{(3)}, X_1^{(3)}, \Delta_1^{(3)}>, \quad (8)$$

где $\varphi_1^{(2)}$ — функция защиты речевой информации от перехвата по прямым акустическим каналам;

$\varphi_2^{(2)}$ — функция защиты речевой информации от съема/передачи;

$\varphi_1^{(3)}$ — функция защиты речевой информации от перехвата в контролируемой зоне;

$A_1^{(3)}$ — информация акустических полей;

$B_1^{(3)}$ — ущерб от нарушения информационной безопасности;

$X_1^{(3)}$ — отсутствие или наличие утечки речевой информации;

$\Delta_1^{(3)}$ — средства защиты речевой информации от перехвата в контролируемой зоне;

$$<\varphi_3^{(2)} + \varphi_4^{(2)} + \varphi_5^{(2)}> = <\varphi_2^{(3)}, A_2^{(3)}, B_2^{(3)}, X_2^{(3)}, \Delta_2^{(3)}>, \quad (9)$$

где $\varphi_3^{(2)}$ — функция защиты речевой информации от перехвата с помощью направленного микрофона;

$\varphi_4^{(2)}$ — функция защиты речевой информации от съема с помощью лазерной акустической системы;

$\varphi_5^{(2)}$ — функция защиты речевой информации от съема за счет ВЧ навязывания;

$\varphi_2^{(3)}$ — функция защиты речевой информации от перехвата вне контролируемой зоны;

$A_2^{(3)}$ — информация акустических полей;

$B_2^{(3)}$ — ущерб от нарушения информационной безопасности;

$X_2^{(3)}$ — отсутствие или наличие утечки речевой информации;

$\Delta_2^{(3)}$ — средства защиты речевой информации от перехвата вне контролируемой зоны;

Функции $\varphi_1^{(3)}$ и $\varphi_2^{(3)}$ третьего уровня композиционной структуры действий по защите речевой информации будут составлять функцию четвертого уровня такого рода структуры (целевую функцию действий по защите):

$$<\varphi_1^{(3)} + \varphi_2^{(3)}> = <\varphi^{(4)}, A^{(4)}, B^{(4)}, X^{(4)}, \Delta^{(4)}>, \quad (10)$$

где $\varphi_1^{(3)}$ — функция защиты речевой информации от перехвата в контролируемой зоне;

$\varphi_2^{(3)}$ — функция защиты речевой информации от перехвата вне контролируемой зоны;

$\varphi^{(4)}$ — целевая функция защиты речевой информации от перехвата по техническим каналам;

$A^{(4)}$ — информация акустических полей;

$B^{(4)}$ — ущерб от нарушения информационной безопасности;

$X^{(4)}$ — отсутствие или наличие утечки речевой информации;

$\Delta^{(4)}$ — средства защиты речевой информации.

Представление функциональных моделей действий по защите речевой информации в виде (1) — (10), позволяет сформировать математическое представление подобного рода действий и создать предпосылки для количественной оценки характеристик механизмов противодействия утечке речевой информации по техническим каналам.

Это дает возможность на основании функционального представления (1) и (2) действий по защите речевой информации сформировать соответствующие выражения для аналитического представления их характеристик:

$$<\varphi_1^{(l)} \,\&\, \ldots \,\&\, \varphi_j^{(l)} \,\&\, \ldots \,\&\, \varphi_J^{(l)}> = <\varphi_k^{(l+1)}, A_k^{(l+1)}, B_k^{(l+1)}, X_k^{(l+1)}, \Delta_k^{(l+1)}> \rightarrow$$

$$\rightarrow \bar{s}_k^{(l+1)} = M\left[s_1 \circ \ldots \circ s_j \circ \ldots \circ s_J\right], \qquad (11)$$

где $\bar{s}_k^{(l+1)}$ — среднее значение характеристики функции $\varphi_k^{(l+1)}$;

$s_j^{(l)}$ — значение одноименной характеристики функции $\varphi_J^{(l)}$;

$\circ$ — знак, обозначающий композицию случайных величин;

$M(\cdot)$ — математическое ожидание от их композиции,

$$<\varphi_1^{(l)} + \ldots + \varphi_j^{(l)} + \ldots + \varphi_J^{(l)}> = <\varphi_k^{(l+1)}, A_k^{(l+1)}, B_k^{(l+1)}, X_k^{(l+1)}, \Delta_k^{(l+1)}> \rightarrow$$

$$\rightarrow \bar{s}_k^{(l+1)} = p_1^l \cdot \bar{s}_1^{(l)} + \ldots + p_j^l \cdot \bar{s}_j^{(l)} + \ldots + p_J^l \cdot \bar{s}_J^{(l)}, \qquad (12)$$

где $p_j^{(l)}$ — вероятность выполнения функции $\varphi_j^{(l)}$;

$\bar{s}_1^{(l)}$ — среднее значение характеристики функции $\varphi_J^{(l)}$.

В результате выполненных исследований с целью аналитического представления информационных процессов и процессов защиты информации получены выражения, соответствующие приведенным в (1) композициям характеристик [5].

С учетом функционального представления (3)—(10) действий по защите речевой информации от утечки по техническим каналам сформируем соответствующее их математическое представление. Для этого воспользуемся форматом преобразований (11), (12) для определения средних значений композиций случайных величин:

$$<\varphi_1^{(1)} \,\&\, \varphi_2^{(1)}> = <\varphi_1^{(2)}, A_1^{(2)}, B_1^{(2)}, X_1^{(2)}, \Delta_1^{(2)}> \rightarrow \bar{s}_1^{(1)} = \int_0^\infty y \int_0^\infty \phi_1^{(1)}(y - y_I)\,\phi_2^{(1)}(y_I)\,dy_I\,dy,$$

где $\phi_1^{(1)}$, $\phi_2^{(1)}$ — плотности распределения случайных величин $s_1^{(1)}$ и $s_2^{(1)}$, соответственно;

$$<\varphi_3^{(1)} + \varphi_4^{(1)}> = <\varphi_2^{(2)}, A_2^{(2)}, B_2^{(2)}, X_2^{(2)}, \Delta_2^{(2)}> \rightarrow \bar{s}_2^{(2)} = p_3^{(1)} \cdot \bar{s}_3^{(1)} + p_4^{(1)} \cdot \bar{s}_4^{(1)};$$

$$<\varphi_5^{(1)} + \varphi_6^{(1)}> = <\varphi_3^{(2)}, A_3^{(2)}, B_3^{(2)}, X_3^{(2)}, \Delta_3^{(2)}> \rightarrow \bar{s}_3^{(2)} = p_5^{(1)} \cdot \bar{s}_5^{(1)} + p_6^{(1)} \cdot \bar{s}_6^{(1)};$$

$$<\varphi_7^{(1)} + \varphi_8^{(1)}> = <\varphi_4^{(2)}, A_4^{(2)}, B_4^{(2)}, X_4^{(2)}, \Delta_4^{(2)}> \rightarrow \bar{s}_4^{(2)} = p_7^{(1)} \cdot \bar{s}_7^{(1)} + p_8^{(1)} \cdot \bar{s}_8^{(1)};$$

$$<\varphi_9^{(1)} + \varphi_{10}^{(1)}> = <\varphi_5^{(2)}, A_5^{(2)}, B_5^{(2)}, X_5^{(2)}, \Delta_5^{(2)}> \rightarrow \bar{s}_5^{(2)} = p_9^{(1)} \cdot \bar{s}_9^{(1)} + p_{10}^{(1)} \cdot \bar{s}_{10}^{(1)};$$

$$<\varphi_1^{(2)} \,\&\, \varphi_2^{(2)}> = <\varphi_1^{(3)}, A_1^{(3)}, B_1^{(3)}, X_1^{(3)}, \Delta_1^{(3)}> \rightarrow$$

$$\bar{s}_1^{(3)} = \int_0^\infty y \int_0^\infty \phi_1^{(2)}(y - y_I)\,\phi_2^{(2)}(y_I)\,dy_I\,dy,$$

где $\phi_1^{(2)}$, $\phi_2^{(2)}$ — плотности распределения случайных величин $s_1^{(2)}$ и $s_2^{(2)}$, соответственно;

$<\varphi_3^{(2)} + \varphi_4^{(2)} + \varphi_5^{(2)}> = <\varphi_2^{(3)}, A_2^{(3)}, B_2^{(3)}, X_2^{(3)}, \Delta_2^{(3)}> \rightarrow \bar{s}_2 = p_3 \cdot \bar{s}_3 + p_4 \cdot \bar{s}_4$;

$<\varphi_1^{(3)} + \varphi_2^{(3)}> = <\varphi^{(4)}, A^{(4)}, B^{(4)}, X^{(4)}, \Delta^{(4)}> \rightarrow \bar{s} = p_1 \cdot \bar{s}_1 + p_2 \cdot \bar{s}_2$.

Рассмотренный способ позволяет сформировать комплекс математических моделей для количественной оценки эффективности различных вариантов построения механизмов защиты информации от утечки по техническим каналам.

ЛИТЕРАТУРА

1. Калянов Г.Н. CASE: Структурный системный анализ (автоматизация и применение). — М.: Лори, 1996. — 242 с.

2. Скрыль С.В., Карпычев В.Ю., Потанин В.Е. Формальные основы функционального моделирования вредоносных воздействий на защищенные информационные системы в интересах выявления противоправных действий в сфере компьютерной информации // Наука производству. — № 3(89). — 2006. — С. 30—31.

3. Советов Б.Я., Яковлев С.А. Моделирование систем: учебник для вузов — 3-е изд., перераб. и доп. — М.: Высшая школа, 2001. — 343 с.

4. Технические средства и методы защиты информации: учебник для студентов высших учебных заведений / С.В. Скрыль [и др.]. — М.: Машиностроение, 2008. — 508 с.

5. Оценка защищенности информационных процессов в территориальных ОВД: модели исследования: монография / В.К. Джоган [и др.]. — Воронеж: Воронежский институт МВД России, 2010. — 217 с.

СВЕДЕНИЯ ОБ АВТОРАХ

Джоган Василий Климович. Доцент кафедры информационно-технического обеспечения.
Воронежский институт ФСИН России.
Россия, 394072, г. Воронеж, улица Иркутская, 1а. Тел. (473) 260-68-19.

Авсентьев Александр Олегович. Адъюнкт кафедры информационной безопасности.
Воронежский институт МВД России.
Россия, 394065, г. Воронеж, проспект Патриотов, 53. Тел. (473) 262-33-76.

Joghan Vasiliy Klimovitch. Assistant Professor of Information Technology Services chair.
Voronezh Institute of Federal Penitentiary Service of Russia.
Work address: 394072, Russia, Irkutskaya Str., 1a. Tel. (473) 260-68-19.

Avsentjev Alexander Olegovich. Post-graduate cadet of Information Security chair.
Voronesh Institute of the Ministry of the Interior of Russia.
Work address: Russia, 394065, Voronesh, Prospect Patriotov, 53. Tel. (473) 262-33-76.

Ключевые слова: функциональная модель, противоправные действия по перехвату речевой информации, функциональная декомпозиция целевой предметной функции.

Key words: functional model, illegal actions for interception of voice information, functional decomposition of the target objective function.

УДК 621.3

Р.А. Солодуха, Д.В. Машуков

ОПЫТ СИГНАТУРНОГО АНАЛИЗА СТЕГАНОГРАФИЧЕСКОЙ ПРОГРАММЫ S-TOOL

THE EXPERIENCE OF THE STEGANOGRAPHY PROGRAM S-TOOL SIGNATURE ANALYSIS

Описан алгоритм работы программы S-Tool по извлечению стегановложения, полученный путем дизассемблирования. Сделаны выводы о возможностях сигнатурного анализа стеганоконтейнеров.

The S-Tool extracting algorithm obtained by disassembling is described. The conclusions about the possibilities of the stego-cover signature analysis are presented.

Введение

В соответствии с [1,2] все известные на настоящий момент методы обнаружения встроенных скрытых методами стеганографии сообщений — методы стеганоанализа могут быть разделены на две группы: методы специализированного стеганоанализа и методы универсального стеганоанализа.

Методы специализированного стеганоанализа ориентированы на обнаружение встроенных сообщений при априори известных методе встраивания и особенностях контейнеров. Наиболее эффективными методами стеганоанализа пространственной области изображения являются: классификация статистик, классификация распределений, RS-стеганоанализ, оценка артефактов компрессии, сравнение центра масс изображения [1,3].

Универсальные методы стеганоанализа ориентированы на выявление нескольких методов стеганографии и обработку контейнера, поступающего в области пространственно-временного представления. Как правило, возможна адаптация к особенностям форматов файлов и новых методов стеганографии. Методы данной группы являются многофакторными, т.е. для проведения стеганоанализа используется набор признаков, а также учёт характера их изменения при встраивании информации для заполненного и пустого стеганоконтейнеров. Наиболее эффективными методом стеганоанализа пространственной области изображения является построение вектора признаков путем последовательного вейвлет-преобразования и обучение с помощью нейросети [4].

Однако можно классифицировать стеганоаналитические методы по аналогии с задачами антивирусной защиты на сигнатурные и эвристические. Все вышеперечисленные методы являются эвристическими, т.е. приблизительными методами обнаружения, которые позволяют с определенной вероятностью предположить, что файл содержит вложение.

В то же время стеганографическое программное обеспечение может быть выявлено путем поиска и анализа определенных характерных особенностей у уже обработанных контейнеров — сигнатур. Любая стеганографическая программа добавляет специальные маркеры в область LSB и анализирует какие-нибудь характеристики контейнера (начальные параметры стеганодетектора) для определения наличия вложения и расчета параметров извлечения. Методы, основанные на поиске сигнатур, достаточно легко автоматизировать, и они могут быть эффективно использованы при обработке большого количества контейнеров без непосредственного участия человека.

Сигнатурные методы — точные методы обнаружения, основанные на знании алгоритма работы стеганодекодера. Естественным недостатком сигнатурного подхода является невозможность выявления новых алгоритмов, информация о которых и соответствующие сигнатуры еще не добавлены в используемую базу знаний стеганоаналитического программного обеспечения.

Сигнатурный анализ стеганографической программы включает в себя два этапа:

1. Определение алгоритма определения наличия вложения (стеганографической программы).

2. Определение параметров вложения (алгоритм, пароль) и его извлечение.

Работа по реализации первого этапа сигнатурного стеганоанализа на примере стеганографических программ S-Tool и StegoMagic путем дизассемблирования. В результате алгоритмы работы стеганодетекторов данных программ восстановлены. Часть работы связанная с программой StegoMagic изложена в [5]. В настоящей статье приводится алгоритм работы S-Tool по извлечению вложения.

Описание и предварительный анализ программы S-Tool

S-Tools (Steganography Tools) — один из лучших и самых распространенных продуктов для платформы Windows95/NT, имеющий статус freeware. Программа позволяет скрывать файлы как в изображениях формата GIF и BMP, так и в аудиофайлах формата WAV. При этом S-Tool сочетает в себе методы стеганографии и криптографии, потому что файл, подлежащий сокрытию, еще и шифруется с помощью одного из криптографических алгоритмов с симметричным ключом: DES, тройной DES или IDEA.

S-Tool использует стандартные библиотеки Windows: ntdll.dll, kernel32.dll, KernelBase.dll, winmm.dll, msvcrt.dll, user32.dll, gdi32.dll, lpk.dll, usp10.dll и другие, возможности данных библиотек можно найти в справочнике по WinAPI. Также используются следующие нестандартные библиотеки:

GIFutil.dll — библиотека для работы с GIF изображениями;

zlib.dll — свободная кроссплатформенная библиотека для сжатия данных;

cryptlib.dll — кроссплатформенная криптографическая библиотека с открытым исходным кодом.

Общая схема осуществления вложения программой S-Tool приведена на рис. 1.

Процесс определения сигнатуры программы S-Tool

Задача заключается в изучении алгоритма работы стеганодекодера программы S-Tool, для чего был использован дизассемблер IDA PRO версии 5.5. Данная программа позволяет превратить бинарный код программы в ассемблерный текст, который может быть применен для анализа работы программы. Так как полный анализ кода программы весьма трудоемок, было принято решение дизассемблировать только те участки кода, которые необходимы для решения поставленной задачи, т.е. работу программы по извлечению вложения с момента ввода пользователем пароля и алгоритма шифрования.

Для определения адреса вызова функции после ввода данных пользователем, была использована программа API Monitor. Используя команду Hook new Process, определили используемые библиотеки и функции в приложении и адрес функции, которая обрабатывает ввод данных пользователя в диалоговом окне «Revealing from».

После ввода данных в диалоговом окне «Revaling form» создается новый поток, в памяти он располагается по адресу 004110B0. По этому адресу вызывается функция _AfxThreadEntry, создающая новый поток. Данный поток отвечает за наличие вложения, извлечение и расшифровку вложения. Функция _AfxThreadEntry возвращает 1 или 0, т. е. код завершения потока (deExitCode). Данное значение передается функции AfxEndThread(DWORD dwExitCode, int), которая решает, продолжить или завершить выполнение данного потока. Функция AfxEndThread вызывается по адресу 0042428A.

Далее по адресу 0040577D вызывается функция UpdateData, которая получает пароль и метод шифрования, введенные пользователем.

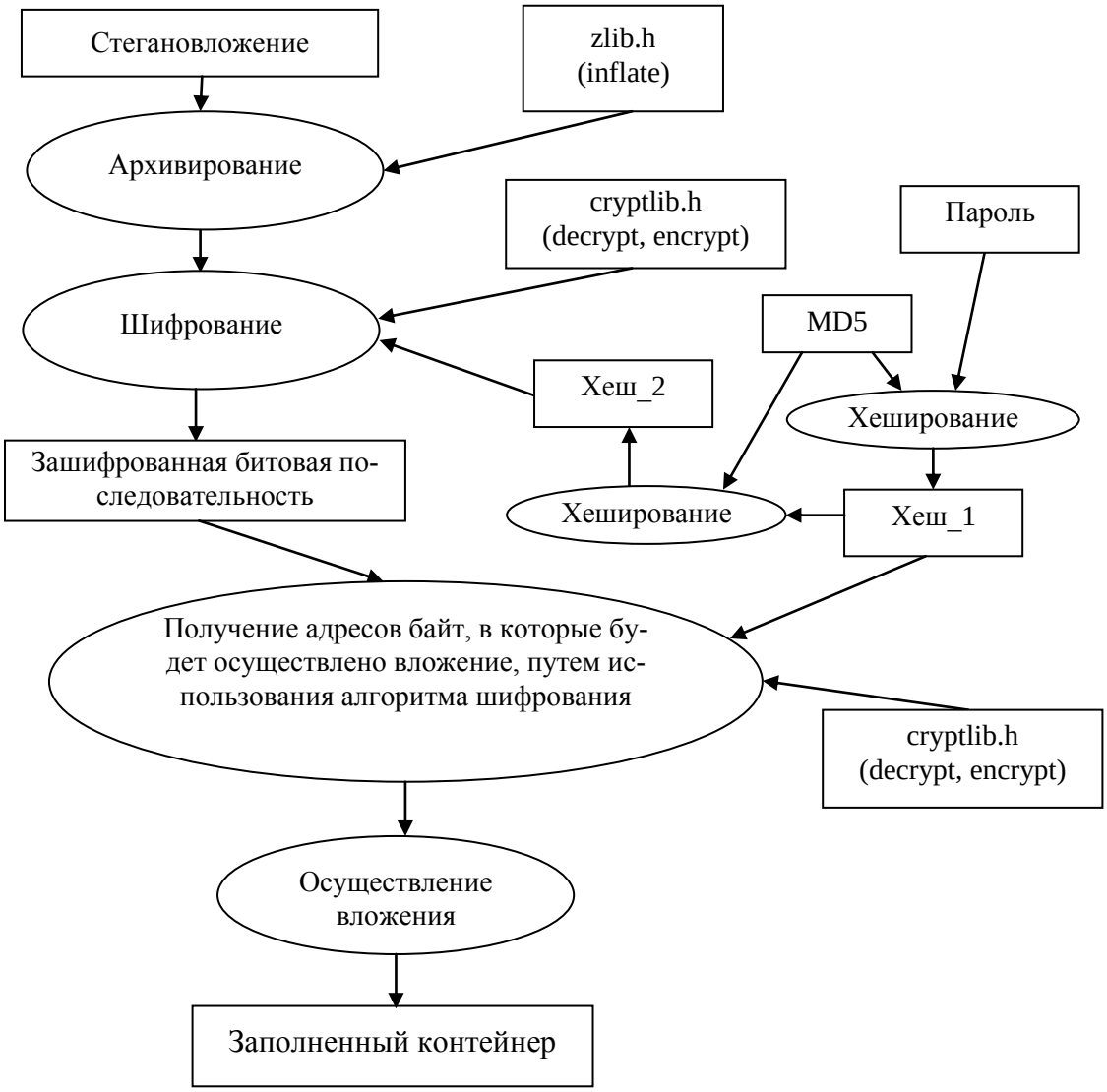

Рис. 1. Общая схема осуществления вложения программой S-Tool

Затем выделятся память, которую условно можно разделить на две части, в первую часть записывается хеш, полученный из введенного пароля с помощью алгоритма MD5, этот хеш равен 128 бит. Во второй части выделенной памяти содержится хеш, полученный из первого хеша. Таким образом, происходит двойное хеширование. Из второго хеша берется столько бит, сколько требуется для выбранного пользователем алгоритма шифрования. Например, для IDEA 128 бит, а для DES 56 бит.

Далее по адресу 004057F9 вызывается функция createMD5, которой передается пароль. Функция возвращает хеш MD5(firstMD5), длина которого 128 бит, полученный хеш сохраняется в выделенную ранее область памяти. Данный хеш используется для нахождения байт контейнера, хранящих биты вложения. Далее полученный хеш хешируется повторно, и, в зависимости от выбранного пользователем алгоритма шифрования, берется нужное количество бит и сохраняется в выделенную ранее область памяти. Данный хеш (secondMD5) будет использоваться для расшифровки вложенного сообщения.

Затем определяется максимальный размер вложения для изображения, начиная с адреса 004018C3 по 004018DF. Максимальный размер вложения в байтах определяется по следующей формуле: Ширина*Высота*3/8 – 16.

Далее по адресу 00406598 вызывается функция queryAlgoModeInformation библиотеки cryptlib.dll, данная функция возвращает объект, описывающий процесс шифрования, передав функции следующие аргументы: режим шифрования CFB и алгоритм шифрования IDEA. Далее по адресу 004057CA вызывается функция loadCryptContext полученного объекта с одним аргументом (firstMD5). Данная функция устанавливает пароль для данного объекта. Этот объект (objAdrEncry) будет использоваться для поиска байт, содержащих биты вложения.

Дальнейший анализ кода внутри созданного потока до вызова функции AfxEndThread показал, что код завершения возвращается функцией, вызывающейся по адресу 00424233. Следовательно, дальнейший анализ нужно продолжить с данной функции. Адрес вызывающейся функции хранится в регистре ECX. Узнав адрес перехода (004110B0), дадим осмысленное название вызванной функции, назовем данную функцию VerificationPsw.

В функции VerificationPsw по адресу 00401B15 вызывается функция FindAdress, которая возвращает адрес в памяти, где хранится bitmap изображения.

Далее выполняется цикл, в котором вызывается функция findAdrBit по адресу 00401B82 с одним аргументом в виде объекта описывающего процесс шифрования. Функция возвращает адрес байта контейнера содержащего один бит размера вложения. Цикл состоит из 64 повторений. Полученные 64 бита располагаются в массиве buff и представляют размер вложения в зашифрованном виде. Функция findAdrBit для поиска адреса использует функцию шифрования encryptBuffer библиотеки cryptlib.dll.

По адресу 00401BE3 вызывается функция InfoDec, которая создает объект, описывающий процесс расшифрования, передав функции режим шифрования CFB и выбранный пользователем алгоритм шифрования. Затем устанавливаем пароль для данного объекта. Пароль — это хеш, полученный повторным хешированием (secondMD5).

Далее по адресу 00401BF4 вызывается функция decryptBuffer библиотеки cryptlib.dll. Аргументом для данной функции является 64 бита зашифрованного размера вложения. Затем расшифрованное значение сравнивается с максимально возможным размером вложения. Если размер вложения не превышает максимального, то размер выделяемой памяти для вложения рассчитывается следующим образом: к расшифрованному значению прибавляем 7h, затем AND 0FFFFFFF8h.

Далее создаем цикл, равный полученному значению, и вложенный цикл, равный 8, формируя, таким образом, зашифрованное вложение побайтно. Адреса байтов контейнера, содержащих вложение определяются по тому же принципу, что и поиск размера вложения.

По адресу 00401D3F вызывается функция decryptBuffer библиотеки cryptlib.dll. Она обрабатывает объект описывающий процесс расшифрования и зашифрованное вложение, на выходе — следующий данные:

путь откуда был загружен файл;

размер сжатого вложения;

размер декомпрессионых данных в байтах;

само сжатое вложение.

Для декомпрессии данных по адресу 00407575 вызывается функция inflate() библиотеки zlib.dll, которой передается сжатое вложение, а возвращается декомпрессионное.

Восстановленный алгоритм работы программы S-Tool по извлечению вложения представлен на рис. 2, 3.

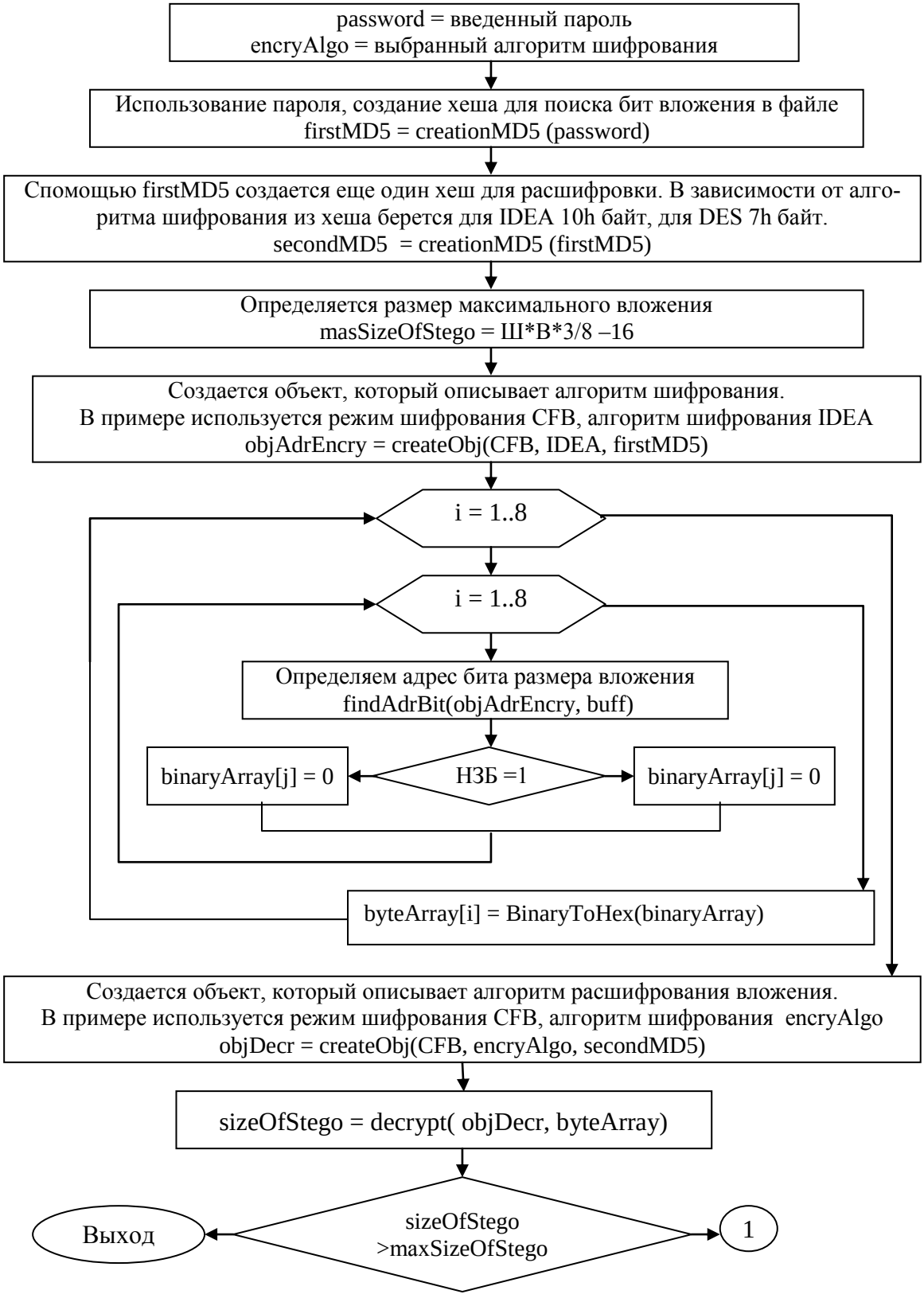

Рис. 2. Алгоритм работы стеганодетектора S-Tool (часть 1)

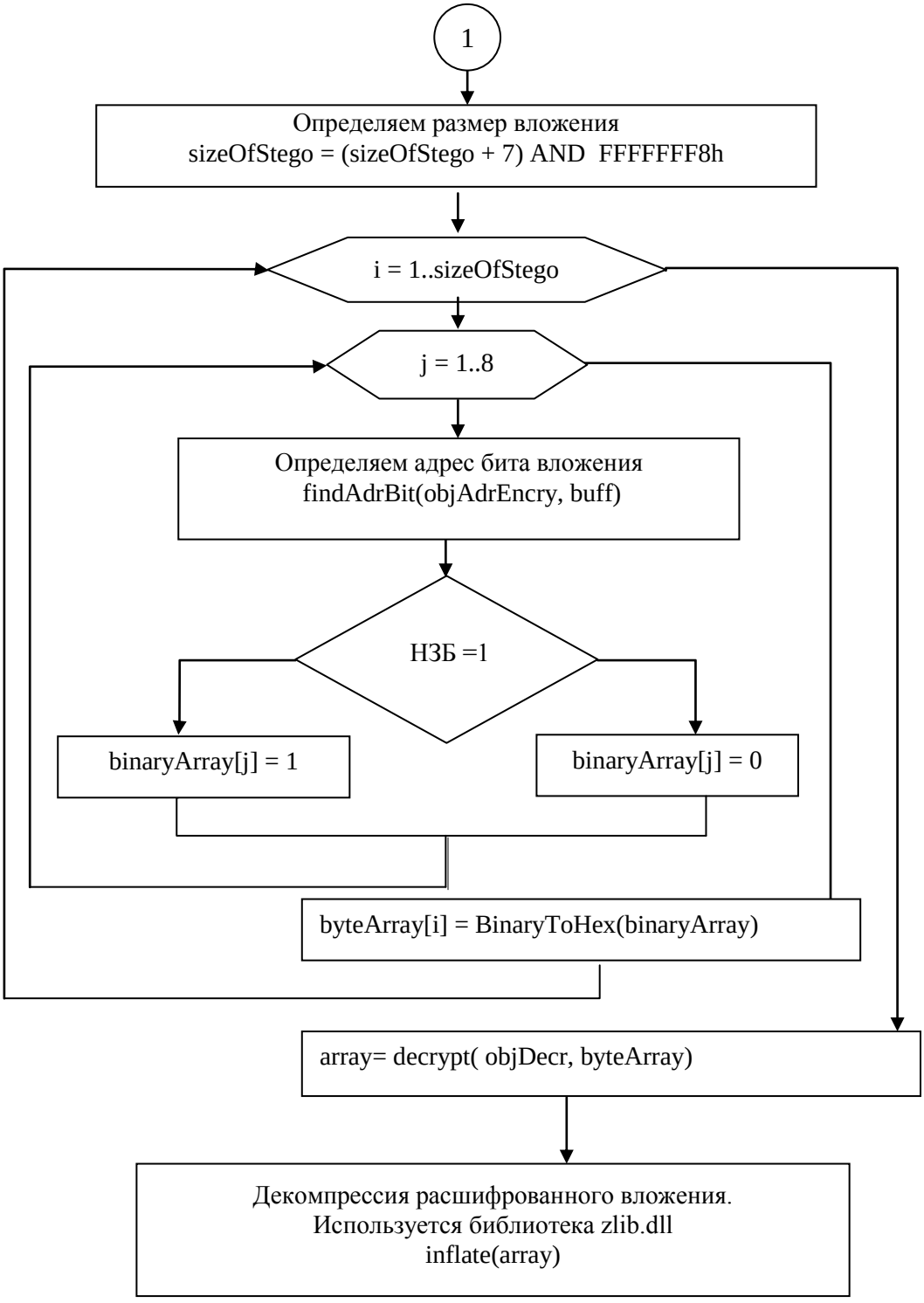

Рис. 3. Алгоритм работы стеганодетектора S-Tool (часть 2)

Заключение

Проведенный анализ алгоритма работы программы S-Tool показал, что определить наличие вложения без знания пароля невозможно, т.к. при определении адресов значащих байт используется библиотека cryptlib.dll с алгоритмом шифрования IDEA

(режим шифрования CFB) и паролем, который вычисляется по алгоритму MD5 на базе введенного пользователем пароля.

Таким образом, S-Tool является более надежной программой, чем StegoMagic, сигнатурный анализ которого вполне возможен. Также данная работа показывает принципиальную невозможность осуществления сигнатурного анализа стеганографических контейнеров, в случае применения разработчиками алгоритма стеганодетектирования, аналогичного S-Tool.

ЛИТЕРАТУРА

1. Стеганография, цифровые водяные знаки и стеганоанализ / А.В. Аграновский [и др.]. — М.: Вузовская книга, 2009. — 220 с.

2. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика. — К.: МК-Пресс, 2006. — 288 с.

3. Швидченко И.В. Методы стеганоанализа для графических файлов // Штучний інтелект. — 2010. —4. — С.697—705.

4. Рублев Д.П. Разработка и исследование высокочувствительных методов стегоанализа: дис. ... канд. техн. наук: 05.13.19 / Юж. федер. ун-т. — Таганрог, 2007. — 139 с.

5. Солодуха Р.А. Опыт сигнатурного анализа программы StegoMagic // Математические методы и информационно-технические средства: труды VIII Всероссийской научно-практической конференции. — Краснодар: Краснодарский университет МВД России, 2012. — С. 210—215.

СВЕДЕНИЯ ОБ АВТОРАХ

Солодуха Роман Александрович. Доцент кафедры автоматизированных информационных систем ОВД. Кандидат технических наук, доцент.

Воронежский институт МВД России.

E-mail: aisovd@vimvd.ru

Россия, 394065, г. Воронеж, проспект Патриотов, 53. Тел. (473) 2623-278.

Машуков Денис Викторович. Оперативный уполномоченный отдела по раскрытию преступлений в сфере высоких технологий.

УВД Гомельского облисполкома Беларуси.

E-mail: denismashukov@mail.ru

Беларусь, г. Гомель, ул. Н. Ополчения, 6/55. Тел. +375(29)1520-864.

Solodukha Roman Alexandrovich. Assistant professor of the automated information systems of interior units chair. Candidate of sciences (technical), assistant professor.

Voronezh Institute of the Ministry of Interior of Russia.

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53. Tel. (473) 2623-278.

Mashukov Denis Victorovich. Detective of high technology crime department.

Department of Interior of Gomel regional executive committee of Belarus.

Work address: Belarus, Gomel, N. Opolcheniya Str., 6/55. Tel. +375(29)1520-864.

Ключевые слова: стеганоанализ; стеганодетектор; стеганодекодер; сигнатурный анализ; метод наименьших значащих бит; дизассемблирование; S-Tool; bmp-файл.

Key words: steganalysis; stegodetector; ctegodecoder; signature analisys; disassembling; S-Tool; bmp-file.

УДК 519.68