ИНФОРМАЦИОННО-ИЗМЕРИТЕЛЬНЫЕ, УПРАВЛЯЮЩИЕ И СЕТЕВЫЕ СИСТЕМЫ

УДК 004.05

ОСОБЕННОСТИ СИНТЕЗА ПОЛНОГО МНОЖЕСТВА ТЕСТОВЫХ СПОСОБОВ УДАЛЕННОГО ИНФОРМАЦИОННО-ТЕХНИЧЕСКОГО ВОЗДЕЙСТВИЯ НА ПРОСТРАНСТВЕННО РАСПРЕДЕЛЕННЫЕ СИСТЕМЫ ИНФОРМАЦИОННО-ТЕХНИЧЕСКИХ СРЕДСТВ

А. А. Бойко, Е. Ю. Обущенко, А. В. Щеглов

ВУНЦ ВВС «Военно-воздушная академия им. проф. Н. Е. Жуковского и Ю. А. Гагарина» (г. Воронеж)

Поступила в редакцию 16.06.2017 г.

Аннотация. Рассмотрено пространство факторов удаленного информационно-технического воздействия (ИТВ) на пространственно распределенные системы информационно-технических средств (ИТС). Приведена методика разработки алгоритмов информационного взаимодействия ИТС в интересах синтеза тестовых способов удаленного ИТВ. Предложен модифицированный метод синтеза тестовых способов удаленного ИТВ на ИТС, базирующийся на представлении ИТС в виде «черного ящика». Показаны исходные данные и результаты автоматического синтеза полного множества тестовых способов удаленного ИТВ на примере процедуры установления соединения сети цифровой радиосвязи, а также язык BOSL для описания этих способов.

Ключевые слова: автоматический синтез, полное множество тестовых способов, удаленное информационно-техническое воздействие, пространственно распределенная система, информационно-техническое средство.

Annotation. Considered the space factors of the remote information-technical impact (ITI) on spatially distributed systems of information-technical tools (ITT). Shown the technique of creating an algorithms of information interaction of ITT interests in the synthesis of test methods of ITV. Proposed a modified method for the synthesis of test methods of ITI on ITT based on the performance of ITT as «black box». Shown the initial data and results of the automatic synthesis of a full set of test methods of ITI on the example for connection establishing procedure of digital radio network, as well as the language BOSL for description of these methods.

Keywords: Automatic Synthesis, Full Set of Test Methods, Remote Information-Technical Impact, Spatially Distributed System, Information-Technical Tool.

ВВЕДЕНИЕ

Сегодня известно множество подходов к обеспечению информационной безопасности пространственно распределенных систем информационно-технических средств[1] (ИТС) в условиях агрессивных удаленных информационно-технических воздействий[2] (ИТВ) злоумышленников. Создаются и поддерживаются в актуальном состоянии базы уязвимостей ИТС [2, 3], активно применяются сканеры защищенности ИТС [4, 5], системы преду-

[1] ИТС – изделие, оборудование, аппаратура или их составные части, функционирующие на основе законов электротехники, радиотехники и (или) электроники, содержащие электронные компоненты и (или) схемы, реализующие одну или несколько следующих функций: усиление, генерирование, преобразование, переключение и запоминание. К ИТС относятся радиоэлектронные средства (РЭС), средства вычислительной техники (СВТ), а также комбинации РЭС и СВТ

преждения и обнаружения ИТВ [6, 7], в ходе разработки пространственно распределенных систем ИТС широко используются средства верификации, в том числе автоматизированного тестирования [8, 9]. Однако ни один из известных подходов в частности или какая-либо их совокупность не могут гарантировать защищенность системы от удаленных ИТВ ввиду неизвестности полного множества таких воздействий.

Получение полного множества тестовых способов удаленного ИТВ на ИТС для доступной информации об алгоритмах функционирования этого средства в пространственно распределенной системе является фундаментальной проблемой теории защиты информации. Ее решение, очевидно, приведет к постепенному разделению пространственно распределенных систем ИТС на две категории: сертифицированные и все остальные. К сертифицированным будут относиться системы, прошедшие проверку, позволяющую обеспечить полную защиту от устранимых уязвимостей, возникших в ходе реализации и потенциально возможных в ходе эксплуатации системы, и дать разработчику информацию о неустранимых уязвимостях. Такая сертификация будет способствовать переходу мировой информационной инфраструктуры на новый эволюционный этап развития, когда разработчики будут проектировать намного более защищенные системы, а устранение уязвимостей реализации и эксплуатации станет «делом техники».

Для решения вышеуказанной проблемы в [10] предложен метод, состоящий в представлении локальных алгоритмов (ЛА) функционирования ИТС (например, базовой станции и абонентского терминала), взаимодействующих в рамках пространственно распределенной системы (например, системы сотовой связи) посредством обмена асинхронными сообщениями, в виде единого распределенного алгоритма (РА), представляемого в виде графа, узлы которого описывают процесс передачи уникальных сообщений. Узел или состояние РА – это совокупность состояния ЛА некоторого ИТС, в котором некоторое сообщение передается, и всех состояний ЛА других ИТС, в котором это сообщение принимается. Переходы графа бывают двух видов:

– прямой переход – из состояния РА C_i ($i = 1 \ldots I$, где I – количество состояний РА) во все состояния РА, у которых состояния ЛА, отправляющие сообщения, без промежуточных входящих сообщений следуют за состоянием, порождающим исходящие сообщения в состоянии РА C_i, или состояниями, получившими входящее сообщение в состоянии РА C_i. Прямые переходы – это легитимные процессы в системе;

– опосредованный переход – из состояния РА C_i во все состояния РА, у которых состояния ЛА, порождающие исходящие сообщения, через одно входящее сообщение следуют за состоянием, порождающим исходящие сообщения в состоянии РА C_i, или состояниями, получившими входящее сообщение в состоянии РА C_i. Опосредованные переходы – это процессы, которые могут быть инициированы злоумышленником и противоречат логике работы системы.

На основе известных параметров информационных элементов[3] передаваемых ИТС сообщений, особенностей ЛА и РА метод позволяет аналитически формировать полное

друг с другом и с другими классами технических средств. См. [1].

[2] Способ ИТВ – последовательность действий, необходимых для формирования совокупности факторов, нацеленных на нарушение конфиденциальности, целостности и/или доступности обрабатываемой ИТС информации и/или алгоритмов ее обработки и достаточных для реализации с использованием электромагнитных полей и/или электрических токов некоторых условий функционирования этого средства, при выполнении которых оно переходит в состояния потери работоспособности, сниженной эффективности функционирования, управляемости и/или доступности для углубленного анализа источником воздействия.

[3] Информационный элемент – это уникальный блок данных, используемый в алгоритмах в качестве самостоятельной единицы, подлежащей обработке (например, поле «адрес отправителя» в сообщении, имя вводимой константы). В [10] информационные элементы называются атомарными предикатами.

множество тестовых способов удаленного ИТВ, учитывающее все потенциально реализуемые наборы взаимосвязанных факторов, влияющих на точность и своевременность сообщений.

При апробации метода выявлен ряд особенностей его применения:

1) ориентация метода на представление системы в виде «белого ящика», характерное, например, для авионики и космонавтики, неудобна и явно избыточна для анализа систем, часто представляемых в виде «черного ящика» (например, при анализе систем связи по спецификациям их протоколов);

2) установлены факты перевода ИТС в целевые для злоумышленника состояния даже с использованием точных и своевременных сообщений, которые в [10] в качестве деструктивных не рассматривались в предположении, что правильность поведения системы не вызывает сомнения. На практике замечены парадоксальные ситуации, когда ожидаемые системой сообщения ей же самой и вредили. Такие ситуации возникали преимущественно при выполнении системой параллельных алгоритмов, верификации темпоральных свойств которых разработчики уделили незначительное внимание, а также при реализации функций обеспечения информационной безопасности ИТС;

3) отсутствие типовой методики разработки алгоритмической модели информационного взаимодействия ИТС в пространственно распределенной системе (алгоритмическая модель – это совокупность ЛА системы), учитывающей критерии их корректности, существенно увеличивало время подготовки исходных данных для синтеза тестовых способов;

4) отсутствие единого языка описания тестовых способов удаленного ИТВ значительно замедляло процесс оценки их эффективности натурным методом, поскольку программные и аппаратные реализации каждого способа значительно отличались.

Настоящая статья имеет целью восполнение вышеуказанных пробелов.

1. УТОЧНЕННЫЙ МЕТОД СИНТЕЗА ТЕСТОВЫХ СПОСОБОВ УДАЛЕННОГО ИНФОРМАЦИОННО-ТЕХНИЧЕСКОГО ВОЗДЕЙСТВИЯ ДЛЯ РАЗЛИЧНЫХ НАБОРОВ ИСХОДНЫХ ДАННЫХ

Необходимо подчеркнуть, что при разработке полного множества тестовых способов удаленного ИТВ рассматриваемым методом имеют место следующие ограничения:

– процесс реализации ИТВ рассматривается без учета вопросов шифрации и дешифрации криптографически защищенных потоков передаваемых по каналам связи данных. Это ограничение обусловлено возможностью применять при необходимости сколь угодно сложные методы и средства дешифрации, исходя из доступных временных и финансовых ресурсов;

– в ходе информационного взаимодействия ИТС рассматривается успешный результат процесса формирования и приема сигналов в виде достоверной последовательности бит, прошедшей приемник ИТС, и учитывается только комплекс преднамеренных деструктивных ИТВ, реализуемых удаленно. Данное ограничение обусловлено ориентацией метода преимущественно на цифровые ИТС, битовые ошибки в которых устраняются известными высокоэффективными программными и аппаратными методами.

Для решения задачи синтеза тестовых способов удаленного ИТВ возможны три варианта наборов исходных данных:

– фолиантный набор, когда доступна только спецификация целевого ИТС. Данный набор исходных данных позволяет вскрыть уязвимости к ИТВ, характерные для целого класса ИТС;

– полевой набор, когда доступны только образцы ИТС. Позволяет вскрыть уязвимости к ИТВ, характерные для конкретных ИТС (вероятность вскрыть уязвимость целого класса ИТС низкая);

– лабораторный набор – комбинация фолиантного и полевого наборов, существенно расширяющая возможности по выявлению уязвимостей в ИТС.

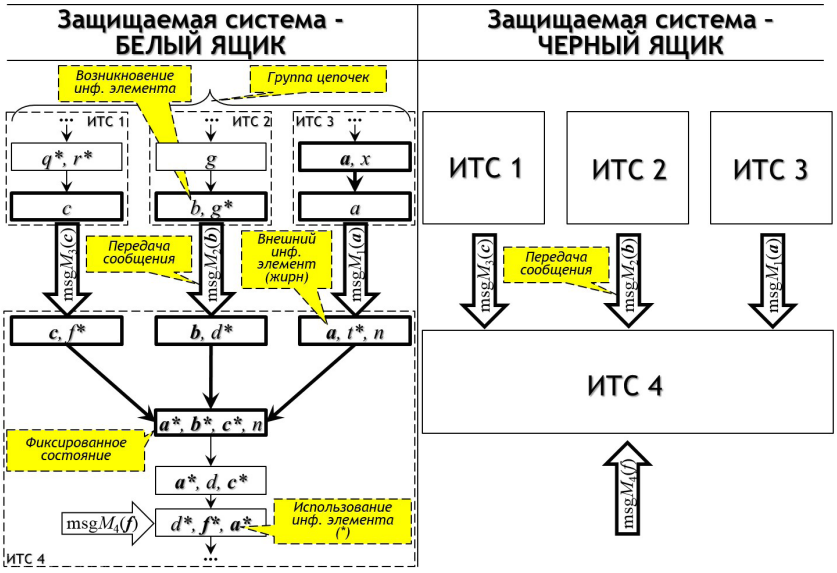

Рис. 1. Фрагмент алгоритмической модели системы

Шаг 1. Выполняют построение всех **локальных алгоритмов** для всех уникальных ИТС пространственно распределенной системы.

Шаг 2. Выполняют **редукцию** локальных алгоритмов.

Шаг 3. Выполняют построение **распределенного алгоритма**.

Белый ящик

Шаг 4. Фиксируют состояния в каждом локальном алгоритме каждого ИТС, непосредственно использующие хотя бы один **внешний инф. элемент** (полученный в сообщении от другого ИТС).

Шаг 5. Определяют для каждого внешнего инф. элемента **цепочку** его прохождения от состояния, в котором он возник (получен, введен), до соответствующего этому инф. элементу зафиксированного состояния.

Шаг 6. Формируют для каждого фиксированного состояния **группу цепочек**, которые содержат используемые в этом состоянии инф. элементы.

Шаг 7. Определяют для каждого вешнего инф. элемента каждого фиксированного состояния **набор тестовых способов ИТВ**, включающий варианты передачи в сообщении этого инф. элемента согласно пространству факторов ИТВ. При проверке одной цепочки в остальных цепочках одной группы принимаются точные и своевременные сообщения.

Черный ящик

Шаг 4. Определяют для каждого инф. элемента, передаваемого в каждом уникальном сообщении, **набор тестовых способов ИТВ**, включающий варианты передачи сообщения согласно пространству факторов ИТВ.

Параметры своевременности сообщений определяют по **распределенному алгоритму**.

Рис. 2. Уточненный метод синтеза полного множества тестовых способов удаленного ИТВ для различных наборов исходных данных

В зависимости от исходных данных о защищаемой системе ее можно рассматривать с позиции «белого» или «черного ящика». Соответствующие примеры фрагмента алгоритмической модели системы показаны на рис. 1.

Фактически для системы, представляемой в виде «белого ящика», возможен анализ состояния всех состояний (блоков) ЛА каждого ИТС и передаваемых в системе сообщений, а система, представляемая в виде «черного ящика», дает возможность анализировать только передаваемые ИТС сообщения.

С учетом этого уточненный метод синтеза полного множества тестовых способов удаленного ИТВ для различных наборов исходных данных можно представить в виде схемы на рис. 2.

Редукция на шаге 2 согласно [10] производится по правилу: каждая последовательность состояний (блоков) ЛА, начинающаяся

после приема (передачи) сообщения и заканчивающаяся перед приемом (передачей) сообщения, заменяется соответствующим этой последовательности состоянием.

2. ПРОСТРАНСТВО ФАКТОРОВ УДАЛЕННОГО ИНФОРМАЦИОННО-ТЕХНИЧЕСКОГО ВОЗДЕЙСТВИЯ НА ПРОСТРАНСТВЕННО РАСПРЕДЕЛЕННЫЕ СИСТЕМЫ ИНФОРМАЦИОННО-ТЕХНИЧЕСКИХ СРЕДСТВ

В дополнение к рассмотренным в [10] факторам точности и своевременности в пространство факторов удаленного ИТВ целесообразно включить фактор кратности. Не смотря на то, что этот фактор рассматривался в [10] в качестве базового по-умолчанию, т.к. эффекты от единичной и N-кратной реализации тестовых способов ИТВ (N определяется экспертно на основе результатов анализа ЛА) могут существенно различаться, постановка акцента на нем будет способствовать наилучшему пониманию и повышению эффективности применения предложенного метода.

С учетом изложенного факторы удаленного ИТВ образуют трехмерное пространство «точность-своевременность-кратность», схематично показанное на рис. 3.

Фактор точности на рис. 3 в сравнении с таковым в [10] дополнен позицией «вне поля точности ожидаемых значений». Необходимость учета этой позиции обусловлена тем, что в ряде случаев информационные элементы отправляемых злоумышленником сообщений могут содержать, например, строковые значения вместо числовых и т. д. Такая особенность фактора точности актуальна, например, для исследования защищенности протоколов высших уровней модели OSI от атак типа SQL-injection. Для низших уровней модели OSI она избыточна, т. к. эти уровни оперируют с единым типом данных.

Фактор своевременности на рис. 3 дополнен позицией «недопущение передачи». Данная позиция в отличие от рассмотренной в [10] позиции «позже» соответствует случаю, когда система сообщение не получит вообще. Актуальность введения новой позиции фактора своевременности обусловлена тем, что эффекты от ИТВ для данных позиций на практике существенно отличаются.

Варианты реализации тестовых способов удаленного ИТВ представлены в табл. 1.

В этой таблице для тестовых способов ИТВ, соответствующих значениям $\gamma = 1\ldots18$ и предполагающих однократную реализацию, дополнительно рассматриваются тестовые способы ИТВ, предполагающие их N-кратную реализацию. В результате количество тестовых способов ИТВ, ориентированных на один информационный элемент, в наиболее общем случае равно 36.

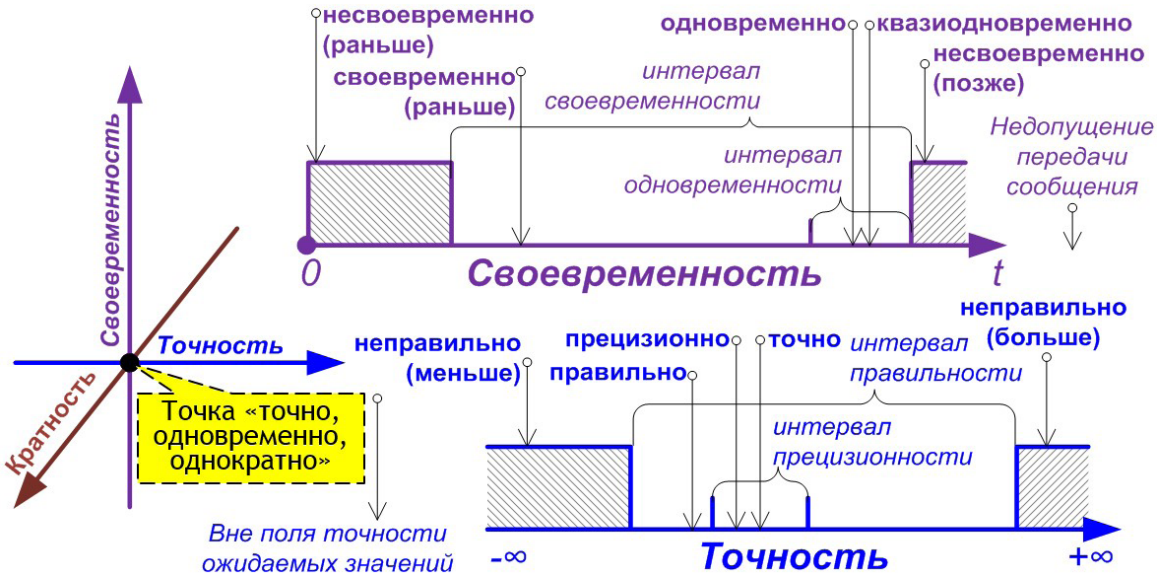

Рис. 3. Пространство факторов удаленного ИТВ

Таблица 1

Варианты реализации тестовых способов удаленного ИТВ

Характеристики сообщений		Номер тестового способа ИТВ γ
Своевременность	Точность	
Своевременно	Точно	1
	Прецизионно	2
	Правильно, но непрецизионно	3
	На нижней границе интервала правильности	4
	На верхней границе интервала правильности	5
	Выше верхней границы интервала правильности	6
	Ниже нижней границы интервала правильности	7
	Вне поля ожидаемых значений	8
Раньше	Точно	9
	Прецизионно	10
	Правильно, но непрецизионно	11
	На нижней границе интервала правильности	12
	На верхней границе интервала правильности	13
	Выше верхней границы интервала правильности	14
	Ниже нижней границы интервала правильности	15
	Вне поля ожидаемых значений	16
Позже	–	17
Недопущение передачи	–	18

3. МЕТОДИКА РАЗРАБОТКИ АЛГОРИТМИЧЕСКОЙ МОДЕЛИ ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ ИНФОРМАЦИОННО-ТЕХНИЧЕСКИХ СРЕДСТВ

Методика разработки алгоритмической модели информационного взаимодействия ИТС в пространственно распределенной системе, необходимой для синтеза тестовых способов удаленного ИТВ, приведена на рис. 4.

Методика предусматривает разработку обобщенного графа функционирования анализируемой системы, в котором узлы – выявленные уникальные процедуры системы, а дуги – возможные переходы между ними. ЛА функционирования ИТС в методике формируются отдельно для каждой уникальной процедуры и отдельно для каждого перехода между процедурами с учетом номенклатуры передаваемых сообщений и информационных элементов. Практика показала, что каждый сформированный ЛА целесообразно проверять на корректность с использованием следующих основных критериев:

– каждому входящему сообщению в любом ЛА должно соответствовать исходящее сообщение в другом ЛА;

– передача сообщений в рамках одного ЛА недопустима;

– каждый переход между блоками ЛА должен начинаться в блоке и заканчиваться в блоке;

– начало и конец перехода в одном блоке недопустимы;

– циклы формируются только с использованием логического блока;

– ЛА должен иметь один начальный блок;

– в случае отсутствия блока завершения (реактивная система) ЛА должен быть зацикленным;

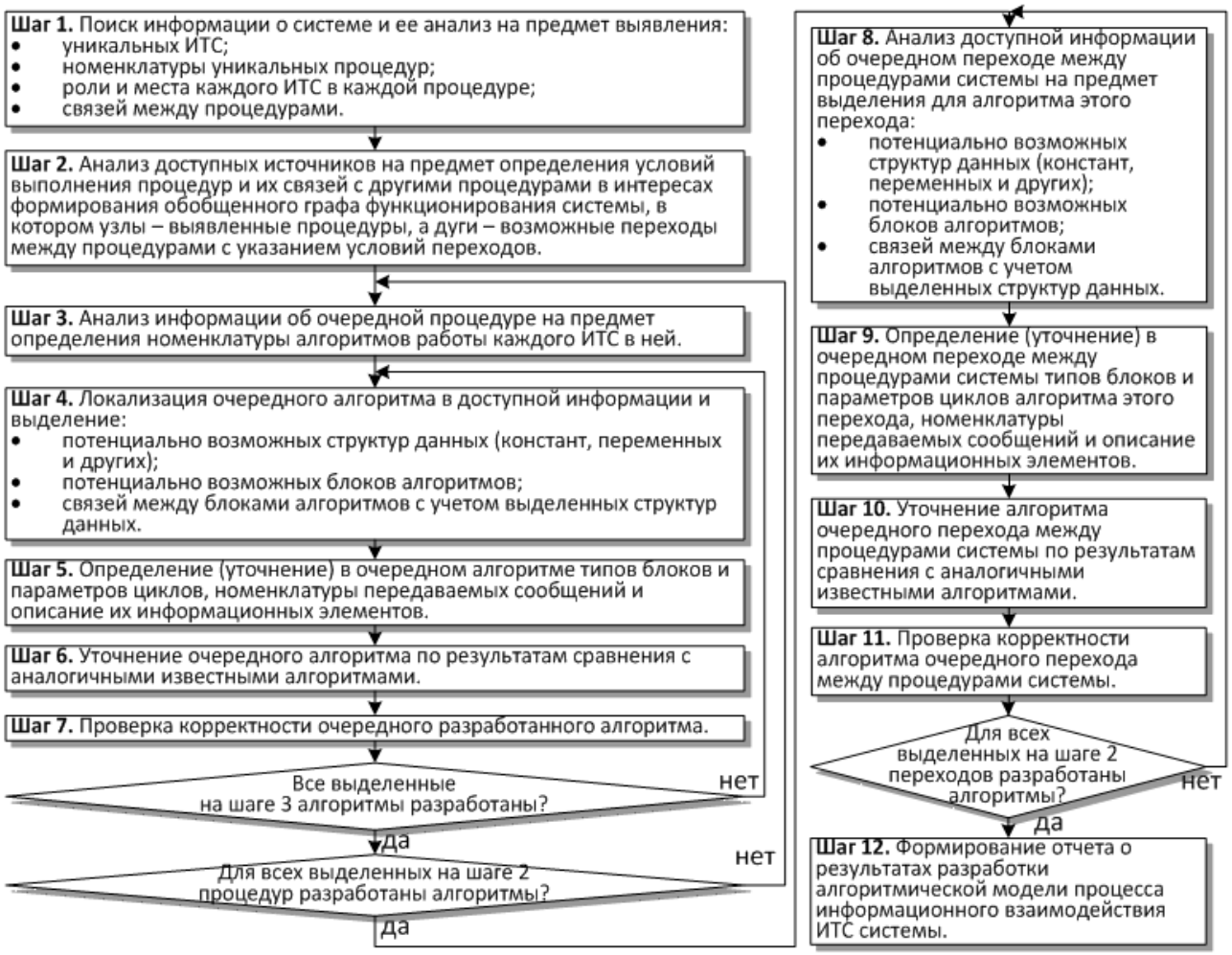

Рис. 4. Методика разработки алгоритмической модели пространственно распределенной системы ИТС

– на пути от возникновения информационного элемента до его использования может быть передача сообщений только между различными ЛА;

– возникновение и/или (использование и/или уничтожение) информационного элемента не должно осуществляться в процессе его передачи в сообщении;

– в каждом блоке может быть только один вход и один или несколько (условный блок) выходов; исключение составляют начальный блок, из которого существует только один выход, и конечный блок, в который может быть более одного входа.

Синтез тестовых способов удаленного ИТВ производится по отдельности для каждой уникальной процедуры и для каждого перехода между процедурами.

4. АВТОМАТИЧЕСКИЙ СИНТЕЗ ТЕСТОВЫХ СПОСОБОВ УДАЛЕННОГО ИНФОРМАЦИОННО-ТЕХНИЧЕСКОГО ВОЗДЕЙСТВИЯ

На практике наиболее сложным шагом рассматриваемого метода для каждого из наборов исходных данных оказался третий шаг – построение РА системы. Даже квалифицированный специалист на данном шаге может допустить до 20 % ошибок при определении опосредованных переходов в РА. Для повышения практичности применения метода авторами разработано и апробировано программное средство, которое автоматически выполняет все следующие за первым шаги метода для вводимых пользователем ЛА функционирования ИТС защищаемой пространственно распределенной системы.

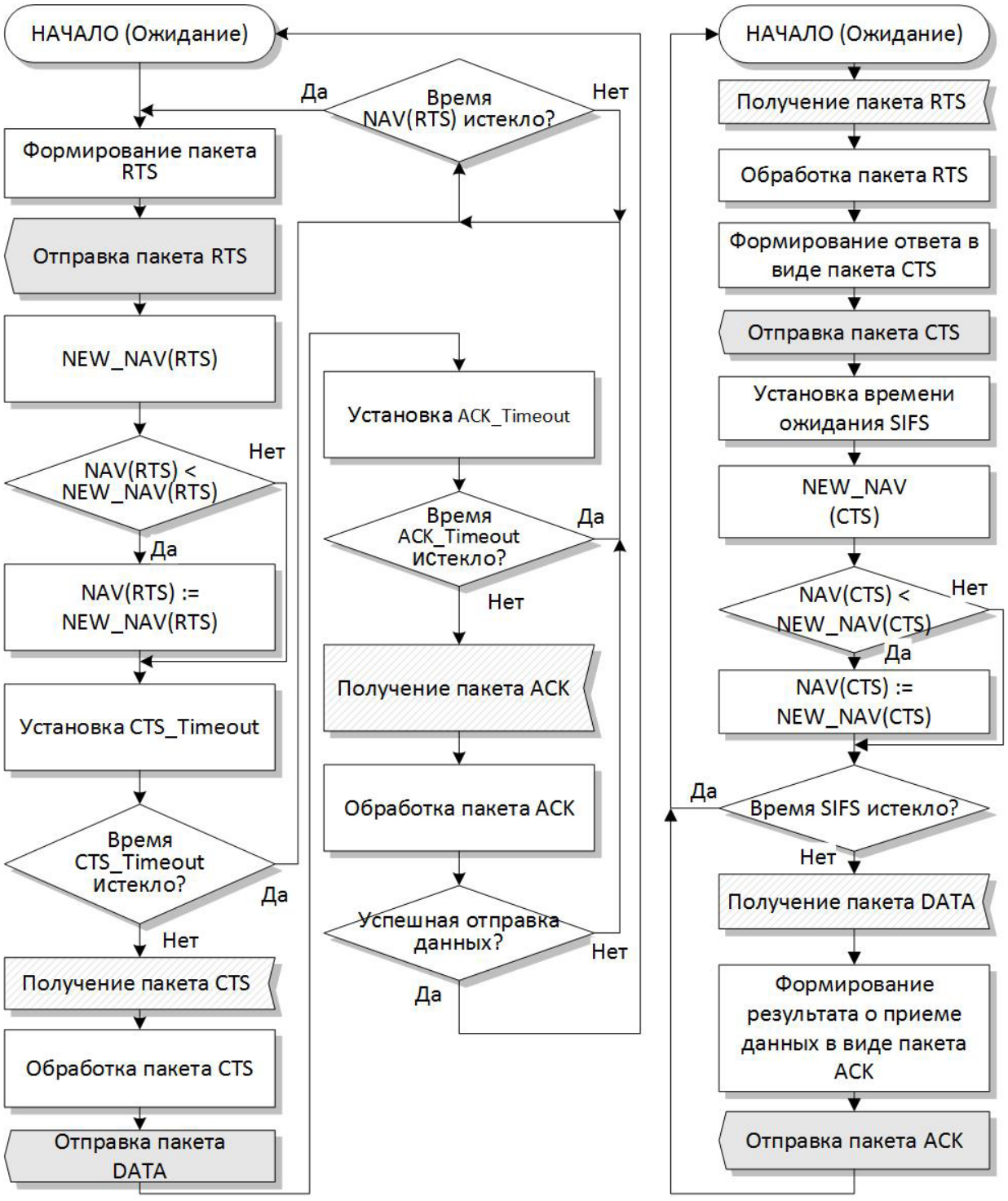

Рис. 5. ЛА функционирования точки доступа (справа) и абонентского терминала (слева) стандарта IEEE-802.11 на уровне процедуры установления соединения для передачи данных

Интерфейс этого программного средства выполнен в стиле продукта Microsoft Visio и позволяет наносить на лист формата А4 состояния (блоки) ЛА с учетом возможности указания связей и названий сообщений и информационных элементов.

Рассмотрим исходные данные и пример результатов автоматического синтеза тестовых способов ИТВ с применением данного программного средства для процедуры установления соединения абонентского терминала с точкой доступа стандарта IEEE-802.11

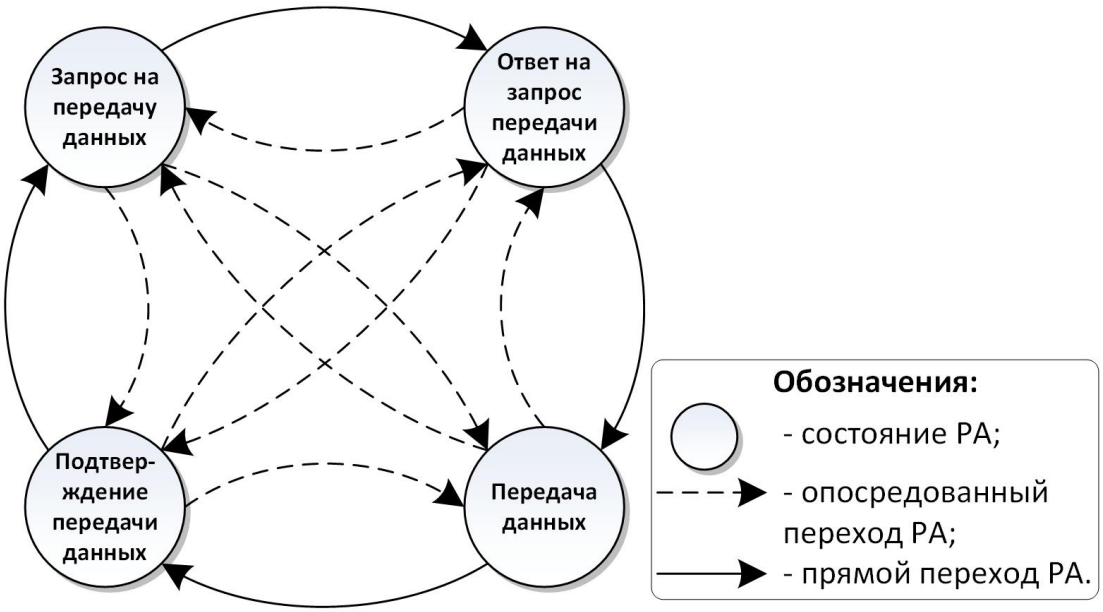

Рис. 6. РА процедуры установления соединения абонентского терминала с точкой доступа стандарта IEEE-802.11

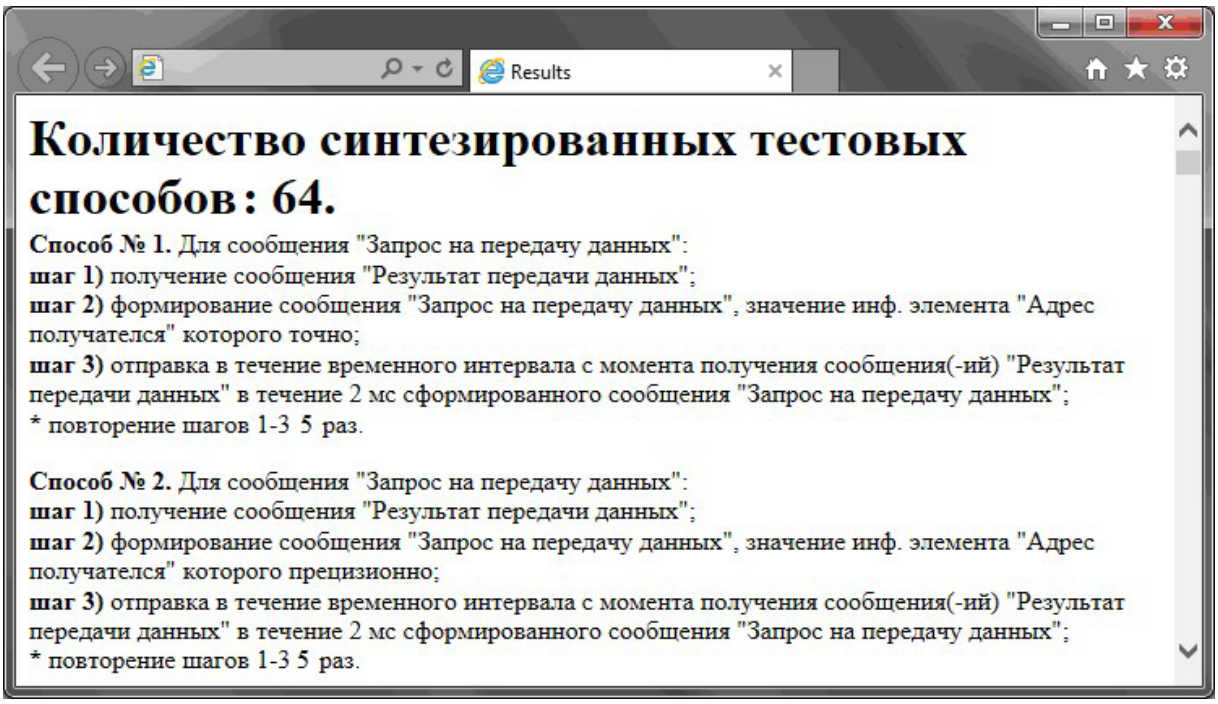

Рис. 7. Фрагмент HTML-файла с результатами синтеза тестовых способов ИТВ

(Wi-Fi) для передачи данных. Описание данной процедуры в полном объеме доступно в спецификации [11]. В примере метод применяется для системы, представленной в виде «черного ящика».

На рис. 5 показаны ЛА функционирования точки доступа и абонентского терминала для рассматриваемого примера, построенные по результатам анализа спецификации [11]. Данные ЛА, а также номенклатура используемых в них сообщений и информационных элементов вводятся в программное средство, после чего по команде пользователя синтезируются тестовые способы удаленного ИТВ.

Для ЛА, показанных на рис. 5, РА имеет вид, представленный на рис. 6. РА программное средство строит в табличном виде.

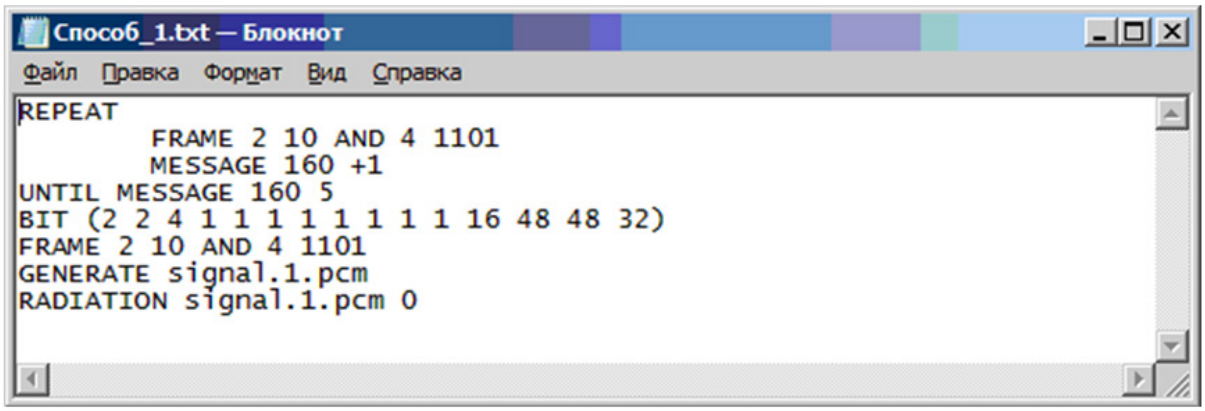

Рис. 8. Пример файла с описанным на языке BOSL способом удаленного ИТВ

После ввода ЛА системы пользователь синтезирует тестовые способы, которые представляются в виде HTML-файла. Фрагмент сгенерированного HTML-файла для рассматриваемого примера приведен на рис. 7.

С учетом изложенного термин «информационно-техническое воздействие», на наш взгляд, является более общим по отношению к часто употребляемому в СМИ и популярной литературе термину «компьютерная атака». Компьютерные атаки, по определению, нацелены на СВТ (compute – от англ. вычислять), а объектами ИТВ являются ИТС. При этом, например, сложная атака «человек посередине» является сценарием применения совокупности разнородных и относительно простых способов ИТВ, аналогичных представленным на рис. 7.

5. ЯЗЫК ОПИСАНИЯ ТЕСТОВЫХ СПОСОБОВ УДАЛЕННОГО ИНФОРМАЦИОННО-ТЕХНИЧЕСКОГО ВОЗДЕЙСТВИЯ BOSL

Программное средство автоматического синтеза тестовых способов удаленного ИТВ представляет их в виде, удобном для последующей оценки эффективности натурным методом. Для этого кроме вышеуказанного HTML-файла для каждого сгенерированного способа создается файл «Способ_X.txt» (где X – номер способа), содержащий последовательность действий, аналогичную представленной на рис. 7, но записанную на специализированном языке описания тестовых способов удаленного ИТВ BOSL (Basic Online Synthesis Language). Команды синтезированных способов на языке BOSL предназначены для трансляции в команды программно-аппаратного устройства, реализующего в режиме реального времени натурный метод оценки эффективности защиты ИТС от тестовых способов удаленного ИТВ, в том числе в интересах оценки эффективности функционирования ИТС с применением математического аппарата, изложенного в [12].

Язык BOSL включает представленные в табл. 2 синтаксические конструкции, описанные с использованием формы Бэкуса-Наура [13].

Пример файла с описанным на языке BOSL тестовым способом показан на рис. 8.

Результаты анализа ИТС различных пространственно распределенных систем показали, что приведенных в табл. 2 конструкций достаточно для реализации любого тестового способа удаленного ИТВ. Поэтому язык BOSL может рассматриваться в качестве претендента на роль унифицированного языка описания тестовых способов удаленного ИТВ для перспективных программно-аппаратных платформ сертификации защищенности ИТС от удаленных ИТВ.

ЗАКЛЮЧЕНИЕ

Таким образом, в настоящей работе получены следующие результаты:

– уточнен метод синтеза тестовых способов удаленного информационно-технического воздействия для информационно-технических средств, представляемых в виде «черного

Таблица 2

Синтаксические конструкции языка BOSL

№ п/п	Форма Бэкуса-Наура синтаксической конструкции	Описание исполняемой команды
1	**<frame>::= FRAMEδ<int>δ<bit> [(+δAND|ORδ<int>δ<bit>)$^{0-n}$]**	Ожидает получение из канала связи сообщения, для которого удовлетворяется до **n+1** условий вида: в сообщении, начиная с бита <**int**>, содержится битовая последовательность <**bit**>. Возможны конъюнкция и/или дизъюнкция условий.
2	**<delay>::= DELAYδ<int>**	Обеспечивает временную задержку перед выполнением следующей синтаксической конструкции на <**int**> мкс.
3	**<repeat>::= REPEATδ<оператор> δUNTILδ<условие>**	Обеспечивает выполнение команды <**оператор**> до тех пор, пока не будет выполнено <**условие**>.
4	**<message>::= MESSAGEδ<int1> [δ<int2>|<+1>]**	Если используется как <оператор>, то накапливает сообщения длиной <**int1**> бит в массив, увеличивая его размер на единицу <**+1**>. Если используется как <условие>, то выдает логическое значение заполненности массива размером <**int2**> сообщениями длиной <**int1**>.
5	**<bit>::= BITδ<int1>δ<int2> [(+δ<int1>δ<int2>)$^{0-n}$]**	Формирует битовую строку **BIT** путем сравнения во всех сообщениях массива <message> до **n+1** последовательности(-ей) бит, начиная с бита <**int1**>, до бита <**int1**>+<**int2**> и записи в строку **BIT** наиболее часто встречающейся(-ихся) в массиве <message> такой(-их) последовательности(-ей). Возможно использование конъюнкции последовательностей.
6	**<modif>::= MODIFδ<int>δ<bit> [(+δANDδ<int>δ<bit>)$^{0-n}$]**	Модифицирует битовую строку **BIT** по **n+1** правилу(-ам) вида: в сообщении биты, начиная с бита <**int**>, заменяются на битовую последовательность <**bit**>. Возможно использование конъюнкции правил.
7	**<generate>::= GENEATEδ<signal.*.pcm>**	Создает файл <signal.*.pcm>, содержащий битовую строку **BIT** передаваемого сообщения.
8	**<radiation>::= RADIATIONδ <signal.*.pcm >δ<int>**	Излучает сообщение из файла <**signal.*.pcm**> с мощностью <**int**> в dBm. Конструкция учитывает параметры передачи сообщения в конкретной физической среде передачи сообщений.

ящика», отличающийся от известного и ориентированного на «белый ящик» введением после построения распределенного алгоритма единственной процедуры определения набора тестовых способов удаленного информационно-технического воздействия для каждого информационного элемента, передаваемого в каждом уникальном сообщении;

– уточнена структура пространства факторов удаленного информационно-технического воздействия на пространственно распределенные системы информационно-технических средств в части: включения фактора кратности в дополнение к факторам точности и своевременности, дополнения фактора точности позицией

«вне поля точности ожидаемых значений» и фактора своевременности позицией «недопущение передачи»;

– предложена методика разработки алгоритмической модели информационного взаимодействия информационно-технических средств в пространственно распределенной системе в интересах синтеза тестовых способов удаленного информационно-технического воздействия, предполагающая разработку обобщенного графа функционирования анализируемой системы, в котором узлы – выявленные уникальные процедуры системы, а дуги – возможные переходы между ними, и локальных алгоритмов информационно-технических средств отдельно для каждой процедуры и перехода с учетом номенклатуры передаваемых сообщений и информационных элементов;

– предложен язык описания тестовых способов удаленного информационно-технического воздействия BOSL (Basic Online Synthesis Language), синтаксические конструкции которого представлены в форме Бэкуса-Наура и предназначены для трансляции в команды программно-аппаратного устройства, реализующего в режиме реального времени натурный метод оценки эффективности защиты информационно-технических средств от данных способов.

Также показаны исходные данные и пример результатов автоматического синтеза тестовых способов удаленного информационно-технического воздействия с применением специализированного программного средства для процедуры установления соединения абонентского терминала с точкой доступа стандарта IEEE-802.11. Полученные результаты могут использоваться при создании перспективных программно-аппаратных платформ сертификации информационно-технических средств на предмет защищенности от удаленных деструктивных информационно-технических воздействий.

СПИСОК ЛИТЕРАТУРЫ

1. *Балыбин В. А.* О терминологии в области радиоэлектронной борьбы в условиях современного информационного противоборства / В. А. Балыбин, Ю. Е. Донсков, А. А. Бойко // Военная Мысль. – 2013. – № 9. – С. 28–32.

2. Common Vulnerabilities and Exposures [Электронный ресурс]. – Режим доступа: http://cve.mitre.org.

3. Банк данных угроз безопасности информации [Электронный ресурс]. – Режим доступа: http://bdu.fstec.ru.

4. Canvas [Электронный ресурс]. – Режим доступа: http://immunitysec.com.

5. Nessus [Электронный ресурс]. – Режим доступа: http://tenable.com.

6. Kaspersky Total Security [Электронный ресурс]. – Режим доступа: http://kaspersky.com.

7. Norton Security Deluxe [Электронный ресурс]. – Режим доступа: http://norton.com.

8. Rational Software Architect [Электронный ресурс]. – Режим доступа: http://www-03.ibm.com.

9. CTESK [Электронный ресурс]. – Режим доступа: http://www.unitesk.ru

10. *Бойко А. А.* Способ разработки тестовых удаленных информационно-технических воздействий на пространственно распределенные системы информационно-технических средств / А. А. Бойко, А. В. Дьякова // Информационно-управляющие системы. – 2014. – № 3. – С. 84-92.

11. IEEE Std 802.11-2012. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. – Режим доступа: https://standards.ieee.org/getieee802/download/802.11-2012.pdf.

12. *Бойко А. А.* Способ стратифицированного аналитического описания процесса функционирования информационно-технических средств / А. А. Бойко // Информационные технологии. – 2015. – № 1. –С. 35-42.

13. *Knuth D. E.* Backus Normal Form vs. Backus Naur Form / Knuth D.E., 1967 – p.p. 735–736.

Бойко А. А. – канд. техн. наук, доцент, начальник отдела, научно-исследовательский испытательный институт, Военный учебно-научный центр Военно-воздушных сил «Военно-воздушная академия им. профессора Н. Е. Жуковского и Ю. А. Гагарина».
E-mail: algeminy@mail.ru

Обущенко Е. Ю. – бакалавр техн. наук, инженер-программист, научно-исследовательский испытательный институт, Военный учебно-научный центр Военно-воздушных сил «Военно-воздушная академия им. профессора Н. Е. Жуковского и Ю. А. Гагарина».
E-mail: jony457@yandex.ru

Щеглов А. В. – бакалавр техн. наук, инженер-программист, научно-исследовательский испытательный институт, Военный учебно-научный центр Военно-воздушных сил «Военно-воздушная академия им. профессора Н. Е. Жуковского и Ю. А. Гагарина».
E-mail: shcheglov95@gmail.com

Boyko A. A. – Candidate of Technical Sciencies, Associate Professor, Chief of Department, Research and Testing Institute, Military Education-Science Center of Military Air Forces "Professor N. E. Zhukovsky and Yu. A. Gagarin Military Air Academy".
E-mail: algeminy@mail.ru

Obushenko E. Y. – Bachelor of Technical Sciencies, Software Engineer, Research and Testing Institute, Military Education-Science Center of Military Air Forces "Professor N. E. Zhukovsky and Yu. A. Gagarin Military Air Academy".
E-mail: jony457@yandex.ru

Shcheglov A. V. – Bachelor of Technical Sciencies, software engineer, Research and Testing Institute, Military Education-Science Center of Military Air Forces "Professor N. E. Zhukovsky and Yu. A. Gagarin Military Air Academy".
E-mail: shcheglov95@gmail.com