Baizdrenko K.A., Bezuglaya A.E., Shushlyapin E.A. Formation of equivalent relay control for non-linear systems using Fourier approximation of transient functions

The article is devoted to the problem of determination of switching moments for limited relay controls in non-linear systems, which provide achievement of system positions in close proximity to conditions, achievable under influence of limited in the same limits arbitrary-shaped controls.

Keywords: relay control, equivalent control, substitution of control.

Байздренко К.О., Безугла А.Є., Шушляпін Є.А. Побудова еквівалентних релейних управлінь для нелінійних систем на основі фур`є-апроксимації перехідних функцій

Робота присвячена завданню визначення моментів перемикання обмежених релейних управлінь для нелінійних систем, що забезпечують досягнення станів системи, близьких до станів, що отримуються під впливом обмежених в тих же межах управлінь довільної форми.

Ключові слова: релейне управління, еквівалентне управління, заміна управління

УДК 004.56

А.В. Скатков, проф., д-р техн. наук
А.А. Брюховецкий доц., канд. техн. наук
Е.Н. Мащенко доц., канд. техн. наук
Ю.П. Николаева
Севастопольский национальный технический университет
ул. Университетская 33, г. Севастополь, Россия, 299053
E-mail: kvt.sevntu@gmail.com

ФУНКЦИОНАЛЬНО-СТРУКТУРНОЕ МОДЕЛИРОВАНИЕ ПРОЦЕССОВ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ НА ОСНОВЕ КРИТЕРИАЛЬНЫХ ДЕТЕКТОРОВ АТАК[7]

Рассматривается задача по разработке системного обеспечения программно-аппаратного комплекса исследовательского стенда, которая может быть решена только на основе системного исследования и анализа задачи оценки мощности статистических критериев идентификации вирусных атак. Представлены результаты экспериментальных исследований оценки эффективности разработанного комплекса.

Ключевые слова: *обнаружение вторжений, критериальные детекторы атак, информационная безопасность.*

Развитие информационных технологий на базе телекоммуникационных сетей (ТКС) приводит к повышению эффективности промышленного производства и многих инфраструктур в энергетической, транспортной, социальной сферах [1]. ТКС, как одна из основных подсистем инфраструктур, должна обеспечивать высокую реактивность, достоверность и своевременность передачи информации между функциональными подсистемами инфраструктуры. Отказ или нарушение работы ТКС может привести к дезорганизации функционирования всей инфраструктуры и, следовательно, опасности возникновения критических ситуаций, которые могут иметь катастрофические последствия. Несмотря на интенсивное развитие компьютерных систем и информационных технологий защиты, ТКС продолжают быть уязвимыми для внешних и внутренних несанкционированных вторжений. Основной угрозой безопасности ТКС являются акты несанкционированного перехвата каналов обмена информацией и управления. Несанкционированный перехват каналов может быть осуществлен в результате нарушения прав доступа субъектов к объектам ТКС.

Актуальность, научная обоснованность и перспективность построения систем обнаружения вторжений обусловлена растущей сложностью и масштабами компьютерных систем и сетей, что в свою очередь приводит к необходимости разработки и созданию новых подходов в решении проблемы обеспечения информационной безопасности.

В статье решается задача оценки системных характеристик ТКС, подвергшихся воздействию вторжений на основе выбора параметров эффективного критериального детектора атак (КДА), которая, в свою очередь, сводится к исследованию мощности статистических критериев [2]. Исследование мощности непараметрических критериев является аналитически неразрешимым. Возникает необходимость разработки и построения информационной технологии специализированного программно-аппаратного комплекса (стенда). Используя данный стенд, представляется возможным исследовать вероятности допущения ошибок первого и второго рода (α и β). На основе полученных

[7] Работа выполнена при финансовой поддержке РФФИ (грант № 14-47-01514).

исследовательских данных возможно построение системы поддержки принятия решений (СППР) в системах управления правами доступа (СУПД).

Для выполнения задачи исследования мощности критериев и построения СППР в СУПД и моделей СУПД необходимо разработать программное обеспечение стенда, включающее модели генераторов случайных чисел, с помощью которых можно получать выборки, близкие к реальным выборкам параметров сложных систем.

Успешное проектирование и разработка системного обеспечения программно-аппаратного комплекса исследовательского стенда может быть достигнуто только на основе системного исследования и анализа задачи оценки мощности критериев идентификации вирусных атак. Для этой цели, требуется реализация следующих функций:

– генерация случайных выборок с априорно заданными параметрами;

– обеспечение возможности исследователю (пользователю программного комплекса) управлять комплексом путем изменения входных параметров;

– обеспечение работы подсистемы проверки случайных выборок на применимость к ним статистических критериев (проверка нормальности случайных выборок);

– обеспечение работы подсистемы вычисления статистических критериев;

– обеспечение работы подсистемы логического вывода о принадлежности вычисленного критерия множеству значений принятия гипотезы;

– анализ статистических вероятностей допущения ошибок первого и второго родов;

– предоставление возможности исследователю (пользователю программного комплекса) получать данные о мощностях исследуемых критериев.

Для обеспечения этих функций, в структуре программного обеспечения выделим элементы, в дальнейшем представляемые как подсистемы, структура взаимодействия которых отображена в виде графа на рисунке 1:

PS1 - подсистема генерации выборок случайных величин;

PS2- подсистема управления генераторами случайных величин и работой программного комплекса;

PS3- подсистема проверки применимости выбранных статистических критериев к выборкам случайных величин;

PS4 - подсистема вычисления статистических критериев;

PS5 - подсистема логического вывода о принадлежности вычисленного критерия множеству значений принятия гипотезы;

PS6 - подсистема анализа статистических вероятностей допущения ошибок первого и второго родов;

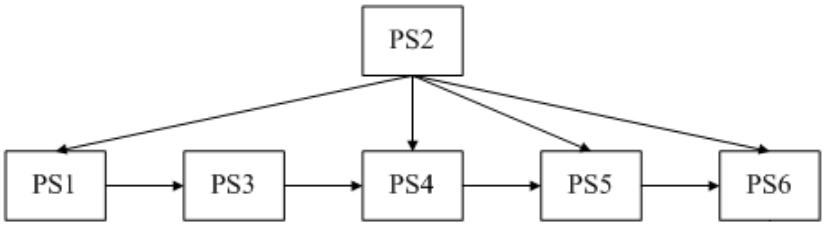


Рисунок 1 – Элементы программного обеспечения исследовательского стенда и связи между ними

Объединение перечисленных подсистем позволит построить единый программный комплекс исследования эффективности статистических критериев.

Проектируемая система может развиваться за счет:

- увеличения скорости вычисления статистических критериев и подсчета статистических вероятностей допущения ошибок первого и второго рода путем оптимизации внутренних структур модулей, а так же использования параллельных и распределенных вычислений;

- пополнения библиотеки исследуемых статистических критериев;

- пополнения методов интеллектуального анализа данных.

В проектируемой системе было выделено множество подсистем. Практически каждую из выделенных подсистем можно разделить на ряд более мелких подсистем и реализовывать как автономные модули. Данный подход делает возможным получение множества автономных исполняемых модулей, что позволит с меньшими затратами разрабатывать новые системы.

С другой стороны, можно объединить все подсистемы в один модуль с целью его применения в системах более высокого иерархического уровня.

Интеграция представленных функций, а так же использование систем ППР, для которых предложенные технологии являются источниками информации, позволяет предложить базовую структуру ИТ критериального обнаружения атак (КОА) (рисунок 2),

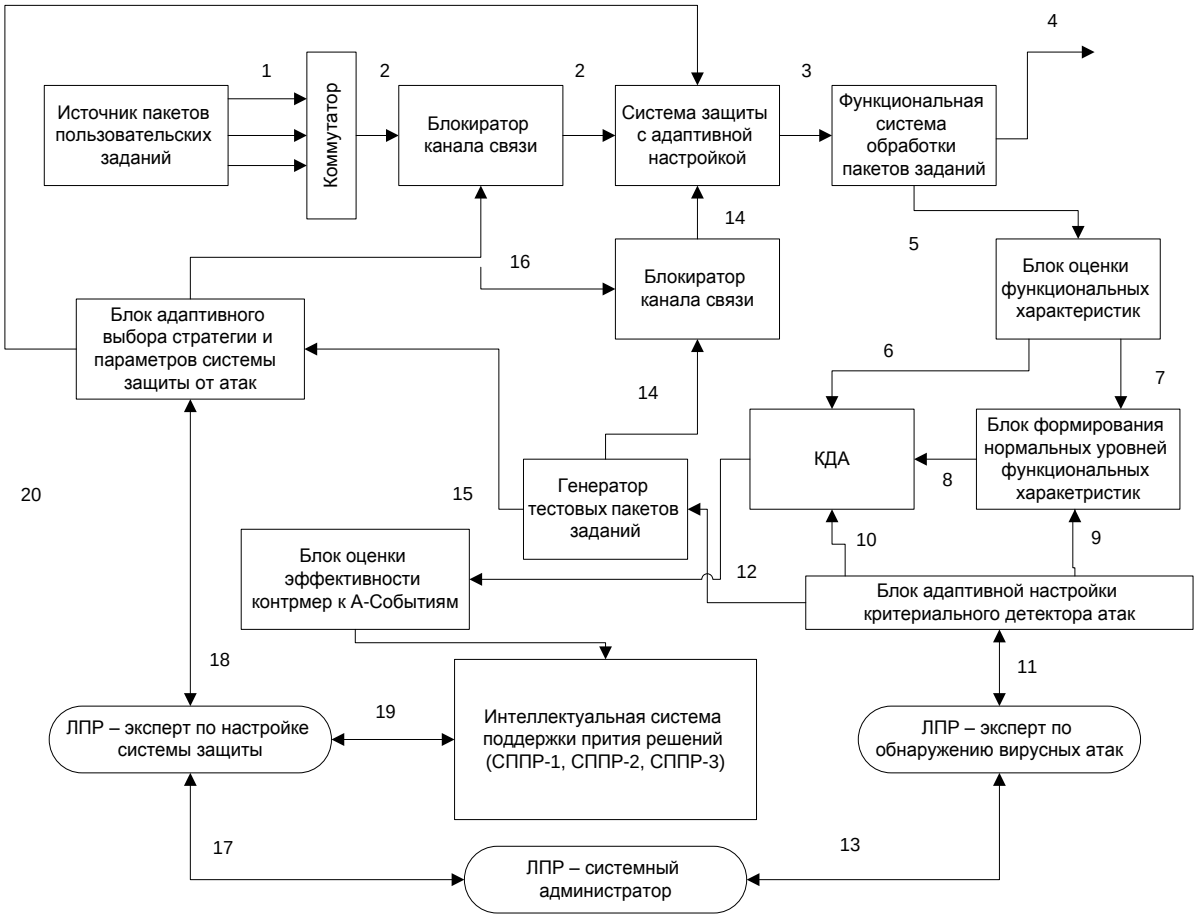


Рисунок 2 – Функциональная схема ИТ критериального обнаружения атак

где 1 – поток пакетов пользовательских заданий; 2 – пакеты пользовательских заданий для обслуживания в конкретном объекте ТКС; 3 – пакеты пользовательских заданий, проверенные на принадлежность к А-событиям на ТКС; 4 – результаты обработки пакетов пользовательских заданий; 5 – функциональные характеристики системы обработки пакетов заданий; 6 – выборки функциональных характеристик; 7 – выборки функциональных характеристик при настройке КДА; 8 – нормативные значения функциональных характеристик; 9 – команда сбора нормативных уровней функциональных характеристик; 10 – параметрическая и структурная настройка КДА; 11 – рекомендации по настройке КДА; 12 – команда начала/окончания генерации пакетов тестовых заданий; 13 –рекомендации по стратегии настройки КДА; 14 – пакеты тестовых заданий; 15 – индикатор работы генератора пакета тестовых заявок;16 – команды блокировки канала связи; 17 – рекомендации по настройке системы защиты ТКС; 18 – настройка системы защиты (изменение интенсивности проверок, типа проверок пакетов и т.д.); 19 – рекомендуемая стратегия защиты для конкретных условий; 20 – команды выбора стратегии защиты.

Возможно выделить несколько базовых сценариев функционирования ИТ КОА. Представим описание сценария обнаружения А-события:

1. Пакет пользовательских заданий (возможно, содержащий атаки или нарушающий права доступа), поступает на обработку в объект ТКС.
2. Коммутатор пакетов пользовательских заявок направляет его на обработку в объект ТКС.
3. Осуществляется проверка пакета в системе защиты с адаптивной настройкой на наличие атак или нарушения прав доступа, согласно заданной политике безопасности.
4. Осуществляется обработка пакета пользовательских задач.

5. Производится оценка вектора функциональных характеристик объекта ТКС, обрабатывающего пакет пользовательских задач.

6. Базируясь на полученном на этапе 5 векторе функциональных характеристик объекта ТКС и нормативных величинах функциональных характеристик, критериальный детектор атак, делает вероятностное предположение о наличии или отсутствии А-события в ТКС.

7. Интеллектуальная система ППР, основываясь на данных, полученных от КДА и настроек, заданных ЛПР, предлагает свои рекомендации о необходимости проведения мероприятий по нейтрализации и противодействию А-событий в ТКС.

Приведенный сценарий может быть расширен за счет процедур получения нормативных значений функциональных характеристик ТКС, оценке эффективности принимаемых к А-событиям контрмер и мероприятий по устранению их действия.

Использование системного подхода позволило получить следующие конструктивные результаты:

1. Установлено, что программный комплекс для исследования мощности статистических критериев является сложной системой. Системообразующим фактором для разрабатываемого программного комплекса является процесс вычисления статистических критериев, что определяет структуру программного комплекса и связи между его подсистемами.

2. Представлены подсистемы и связи между ними. Определены границы программного комплекса от внешней среды. Все множество подсистем системы определяет ее границы, остальные элементы будут внешней средой для системы. Элементы внешней среды могут иметь связи с системой или могут их не иметь. Если такие связи будут обнаружены, то они будут или входными, или выходными, или управляющими сигналами системы.

3. Установлены функции задачи исследования, мощности статистических критериев, выделена структура программного комплекса и связи между элементами структуры. Данные результаты необходимо использовать в дальнейшем для разработки и программирования исследовательского программного комплекса.

4. Определены функции подсистем, которые следует учитывать при разработке подпрограмм комплекса, что позволит повысить точность вычислений в целом.

5. При дальнейшем совершенствовании программного комплекса следует руководствоваться накопленным к этому моменту опытом его эксплуатации.

6. Системный анализ показал, что необходимо учитывать неопределенности во входных данных, позволяющие избежать некорректной работы комплекса.

На основе результатов системного анализа задачи моделирования, получены все необходимые данные для программного комплекса для исследования мощности статистических критериев.

Анализ эффективности информационной технологии критериального обнаружения атак проведен путем моделирования тестовых ситуаций, для чего было разработано семейство имитационных моделей узлов ТКС, учитывающих различные структуры, функциональное назначение, характер развития, последствия атак. Проведено исследование эффективности предложенных ИТ в ТКС, а так же динамической оценки системных характеристик ТКС в условиях наличия А-событий.

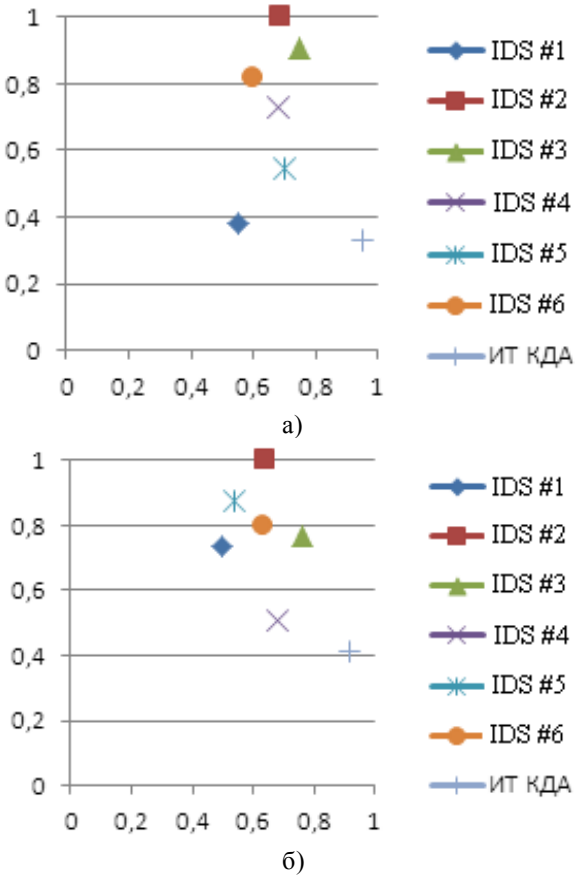
Имитационная модель состоит из следующих блоков: блок генерации пакетов пользовательских заданий, блок обработки пакетов пользовательских заданий, блок обнаружения А-событий, блок оказания противодействия А-событиям, блок восстановления функциональных характеристик ТКС после А-события.

Сравнение предложенной ИТ КОА и известных средств обнаружения А-событий по быстродействию и достоверности в ТКС производилось на компьютере следующей конфигурации: процессор Intel Core 2 Duo E8400 3 ГГц, материнская плата Gygabyte GA-G31MF-S2, видеокарта NVIDIA GeForce 9600 GT, 2 гигабайта оперативной памяти, жесткий диск WDC WD2500JS-22NCB1 (2 шт.), операционная система Microsoft Windows 7 Home Premium x86. В ходе исследования были проанализированы пакеты мультитиповых пользовательских задач с внедренными в них активными вирусными программами.

Пример одного из результатов экспериментальных исследований оценки эффективности ИТ КОА для одного из основных типов пользовательских задач и атак типа «Trojan», «Spyware» представлен на рисунке 3. Результаты проведенных исследований эффективности приведены в Приложении В. В качестве меры эффективности выбран вектор оценок <tоб,S(P(H1|H1))>, где tоб – относительное среднее времени обнаружения наличия А-события, S(P(H1|H1)) – достоверность обнаружения атаки.

Эффективность ИТ зависит от характера поведения вируса, структуры ТКС, характеристик используемых в ТКС программного и аппаратного обеспечения. Проведена оценка эффективности предложенных в работе методов. Внедрение предложенных в данной работе информационных технологий обнаружения атак, использование описанных систем ППР по управлению рисками, ИТ

оценки эффективности принимаемых к А-событиям контрмер уменьшают время обнаружения атак на 13-50% при обеспечении требуемого уровня достоверности.



а)

б)

Рисунок 3 – Относительное среднее время обнаружения наличия А-события а)типа «Trojan», б) типа «Spyware».

Выводы. Для решения задачи оценки системных характеристик ТКС, подвергшихся воздействию А-событий, использовались развитые методы параметрической и структурной идентификации, основанные на аналитической модели многоэтапной деградации и восстановления функциональных характеристик. Данный подход позволил повысить эффективность распределения ресурсов, необходимых для устранения последствий А-событий, и сократить время восстановления до 20%. Предложена структурно-функциональная схема инструментальных средств для реализации системы ППР по анализу и синтезу критериальных детекторов атак.

Библиографический список использованной литературы

1. Информационные технологии для критических инфраструктур: моногр./ Под ред. А.В.Скаткова — Севастополь. СевНТУ, 2012. — 306с.

2. Анализ мощности непараметрических критериев при оценивании состояния объектов критического применения / А.В. Скатков, К.Н. Маловик, Л.П. Луговская, В.С. Ловягин // Научно технический журнал «Радиоэлектронные и компьютерные системы», Выпуск 6 (58), Харьков: изд-во НАУ «ХАИ», 2012г – С. 271-275

Skatkov A.V., Bryukhovetskyi A.A., Mashchenko E.N., Nikolaeva Y.P. Functional-structural modeling intrusion detection basis of acriteria attack detection.

We consider the task of developing a system-software complex, which can be solved only on the basis of a systematic study and analysis of the problem of statistical power estimation criteria for the identification of virus attacks. The results of experimental studies evaluating the effectiveness of the developed complex.

Key words: intrusion detection, criterial detectors attacks, information security.