2. Брайсон А. Новые идеи по теории управления / А. Брайсон // Аэрокосмическая техника. —1986. —№8.— С. 59—75.

3. Воронов А.А. Теория автоматического управления. Ч. II. Теория нелинейных и специальных систем автоматического управления. / А.А. Воронов, Д.П. Ким, В.М. Лохин и др.; Под ред. А.А. Воронова. — М.: Высш. шк., 1986. — 504с.

Барабанов О.Т., Солдатенко О.С. Абсолютна стійкість квазіоптимальної нелінійної системи

Розглядається квазіоптимальна нелінійна система при законі управління, побудованому лінійно-квадратичною оптимізацією системи лінійного наближення. Ставиться і вирішується завдача аналізу абсолютної стійкості в квазіоптимальній системі при парціальному введенні нелінійностей.

Ключові слова: нелінійна система, оптимальний закон керування, абсолютна стійкість, критерій Попова.

Barabanov A.T., Soldatenko E.S. Absolute stability of quasi-optimal nonlinear system

The quasi-optimal nonlinear system with control law, constructed by linear-quadratic optimization for the linear approximation, is considered. The problem of absolute stability analysis in quasi-optimal system with a partial introduction of nonlinearities is posed and solved.

Keywords: nonlinear system, optimal control law, absolute stability, criterion of Popov.

УДК 004.56

А.А. Брюховецкий доц., канд. техн. наук
А.В. Скатков, проф., д-р техн. наук
Д.Ю. Воронин, канд. техн. наук
В.С. Ловягин, канд. техн. наук
Севастопольский национальный технический университет
ул.Университетская 33, г. Севастополь, 299053
e-mail: kvt.sevntu@gmail.com

МЕТОДОЛОГИЯ ПОСТРОЕНИЯ СИСТЕМ ОБНАРУЖЕНИЯ СЕТЕВЫХ ВТОРЖЕНИЙ В КОМПЬЮТЕРНЫХ СЕТЯХ[15]

Представлен комплексный подход к построению систем обнаружению сетевых атак, который сочетает две дополняющие друг друга технологии. Первая позволяет распознавать угрозы сетевых вторжений и базируется на методах интеллектуального анализа данных, в то время как вторая использует информацию об изменении состояния вектора системных показателей компьютерной сети.

***Ключевые слова**: обнаружение сетевых атак, информационная безопасность критических систем.*

В статье представлена методология построения систем обнаружения сетевых вторжений (СОВ) в компьютерных сетях. Применение методологической схемы разработки СОВ обеспечивает воспроизводимость полученных результатов, позволяет создавать опытные образцы перспективных программно-инструментальных средств обнаружения и распознавания сетевых атак для обеспечения информационной защиты компьютерных систем, подготавливает почву для перехода на новый уровень исследований в рамках ОКР.

Анализ проблематики решения фундаментальной задачи обеспечения информационной безопасности на основе методов построения систем обнаружения вторжений в телекоммуникационных сетях показал, что:

- Развитие информационных технологий на базе телекоммуникационных сетей (ТКС) приводит к повышению эффективности промышленного производства и многих инфраструктур в энергетической, транспортной, социальной сферах.
- 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.

Кроме того, известным из литературных источников СОВ [1 — 2] присущи следующие недостатки:

- ограничиваются решением отдельных задач и не носят комплексный характер,

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

- не гарантируют удовлетворительного уровня достоверности обнаружения вторжений в реальных условиях, когда имеет место дефицит априорной информации о свойствах источника вторжений и стохастическая природа распознаваемых событий,
- не обеспечивают возможность распознавания атак на ранних стадиях обнаружения, классификации событий при малых выборках, принятия решений в условиях нестационарного трафика,
- известные модели не дают ни четких ответов, ни рекомендаций по ряду ключевых вопросов, например, как выбирать параметры наблюдения и настройки, как устанавливать границы для шкал измерения параметров, как оценивать достоверность контроля трафика при малых выборках и другие.

К настоящему времени концепция защиты информации изложена в различных источниках [3 — 4]. Однако следует отметить, что и до сегодняшнего дня системная реализация всей совокупности положений концепции сдерживается рядом серьезных трудностей, обусловленных следующими причинами:

1. Значительным своеобразием систем и процессов защиты информации, связанным с повышенным влиянием случайных факторов, в силу чего методы классической теории систем далеко не всегда адекватны характеру моделируемой ситуации, методы же, которые могли бы в достаточной мере дополнить существующие, в необходимой степени не разработаны.
2. Недостаточно четкой проработкой инструментальных средств решения задач анализа и синтеза систем и процессов защиты информации.
3. Недостаточностью, а в ряде случаев отсутствием значительной части исходных данных, необходимых для обеспечения решения названных задач.

В указанных выше публикациях обсуждены возможные пути преодоления данных трудностей, однако конкретные разработки удалось произвести лишь частично.

На основе проведенного анализа известных методов и средств обнаружения сетевых вторжений (акты несанкционированного доступа и вирусные атаки – А-события) в ТКС предлагаются следующие основные перспективные направления синтеза эффективных детекторов и решающих правил:

1. Развитие и совершенствование адаптивных интеллектуальных методов обнаружения вторжений на основе анализа информации сетевого трафика. Данное направление характеризуется достаточно высокой достоверностью обнаружения А-событий, а так же возможностью обнаружения неизвестных ранее типов. К недостаткам этих методов следует отнести: потребность в высоких вычислительных мощностях, сравнительно длительное время обнаружения А-события.

2. Развитие и совершенствование классических методов, основанных на статистическом анализе данных, с использованием критериального обнаружения атак. Данный метод базируется на оценке изменения состояния системных показателей ТКС. Детекторы, построенные на основании данного метода, позволяют за сравнительно небольшой временной промежуток с заданным уровнем достоверности определить наличие А-события в ТКС, в том числе ранее неизвестного типа или вида. Недостаток: трудно обнаруживаются вторжения, которые приводят к незначительным, медленным изменениям системных показателей ТКС.

СОВ представляет собой набор компонентов, связанных общими целями, задачами, структурными отношениями разной природы, технологией обработки информации и информационного обмена. Совокупность этих компонентов представляет собой единую сложную систему, где в состав большинства компонентов может входить человек, вносящий неопределенность в вопросах принятия решений по защите информации. Поэтому разработка формализованной схемы построения СОВ позволит повысить достоверность уровня классификации состояний трафика, распознавание атак на ранних стадиях обнаружения, снижение числа ложных тревог, классификации событий при малых выборках, принятие решений в условиях дефициты априорной информации и нестационарного трафика.

В настоящее время отсутствует единая методология построения СОВ. Многие принимаемые решения носят эвристический характер и недостаточно аргументированы. С целью преодоления данной проблемы в работе предложена совокупность методов, моделей, информационных технологий, интегрированных в единый методический комплекс, в который входят:

- методика построения областей эффективных критериальных детекторов атак, методика получения Парето-эффективных стратегий принятия решений по оценке рисков, методика оценки эффективности распределения ресурсов, необходимых для устранения последствий А-событий;
- методика построения адаптивных систем интеллектуальной поддержки принятия решений на основе решающих правил, с использованием технологии динамического формирования значений метрик, оценки уровня достоверности распознавания состояния сетевого трафика и ошибок первого и второго рода, определения периодов модификации базы правил и др.

Процесс разработки методологии построения СОВ может быть представлен в виде упорядоченной последовательности этапов, которые образуют целостную систему с четко определенными целями, задачами, функциями и структурой.

Методология построения СОВ на основе анализа сетевого трафика включает совокупность приемов, методов, способов и принципов научно-технической деятельности, применяемой для обнаружения сетевых вторжений. Процесс разработки программно-инструментального комплекса, обеспечивающего информационную защиту ТКС, представляет собой исследования по проектированию различных моделей, подходов, методик процесса разработки СОВ, а также изучению основных фаз этого процесса: формирование требований, целей, задач, функций подсистем и их связей, обучение, настройка, адаптация и тестирование модели.

Применительно к разрабатываемой СОВ предлагаемая методология соответствует общепринятым схемам проектирования «сверху вниз» и «снизу вверх» и включает следующие этапы:

- проведение аналитического обзора по открытым научно-техническим источникам и патентам, формулировка постановки задач;
- анализ возможных архитектурных решений и предварительное сравнение их моделей;
- выбор, изучение и проверка качества распознавания базы знаний с прецедентами сетевых атак по выделенным признакам;
- уточнение состава признаков путем исследования их информативности;
- выбор системы интеллектуальных инструментальных средств для анализа сетевого трафика (метрики, параметры, критерии, алгоритмы) и методов обучения для обнаружения и распознавания;
- выбор модульной архитектуры адаптивной СОВ (первый модуль – контроль изменения состояния системных показателей с помощью КДА, второй модуль – распознавание типа атаки на основе интеллектуальных методов обнаружения вторжений);
- программная реализация основных алгоритмов инструментальных средств и решение задач анализа трафика с целью исследования основных характеристик СОВ: вероятность обнаружения вторжений, влияние объемов обучающих выборок на точность результатов, определение периодов модификации решающих правил и др;
- разработка программы и методик испытаний системы;
- проведение экспериментальных исследований (оценка достоверности результатов, анализ ошибок первого и второго рода и т.д.).

Концепция построения СОВ, которая базируется на решении первоочередных научных задач, на наш взгляд, включает:

1. Совершенствование комбинированных методов обнаружения вторжений, включающих в себя адаптивные методы, интеллектуальную логику, статистические методы, позволяющих повысить эффективность СОВ комплексно.

2. Повышение устойчивости адаптивных методов классификации событий в условиях дефицита априорной информации о свойствах источника вторжений и в условиях нестационарного сетевого трафика. Применение таких методов позволит минимизировать число ложных тревог при изменениях сетевого трафика.

3. Повышение эффективности СОВ путем использования моделей, включающих в себя процедуры обучения как средство реализации адаптивного подхода. В основе такого подхода могут быть, например, использованы генетические алгоритмы (ГА). Известно, что классические ГА и их разновидности не всегда применимы при решении задачи мультимодальной оптимизации. Поэтому в таких условиях целесообразно расширить методы ГА использованием подходов искусственных иммунных систем, которым присущи такие свойства как, распознавание, использование принципа необходимого разнообразия, обучение, метадинамика и другие.

4. Разработку систем, в структуре которых содержатся модули адаптации, модификации правил принятия решений, динамического формирования оценок качества правил классификации событий, поддержки принятия решений, которые позволят получить более эффективные в смысле Парето решения задач распознавания вторжений.

5. Разработку методов статистической обработки на основе анализа изменения состояния вектора системных показателей, базирующихся на критериальном обнаружении атак.

6. Применение методов имитационного моделирования, которые позволяют восполнить дефицит априорной информации об источнике вторжений, оценить достоверность принимаемых решений, получить оценки ошибок первого и второго рода.

В основе концепции лежит комплексный подход построения систем обнаружения вторжений. Структурная схема концепции защиты ТКС приведена на рисунке 1.

В целях создания предпосылок для построения адекватных моделей защищаемых информационных систем и технологий требуется разработать методологию их структуризации. Для обеспечения объективной оценки уязвимости информации необходимо сформировать: систему показателей уязвимости, систему угроз информации, методы и модели определения и прогнозирования значений показателей уязвимости. Для формализации решений по защите информации требуется определить: функции защиты; задачи защиты;

выбор средств защиты, с помощью которых решаются задачи, и наконец, построение системы защиты, представляющей собой организованную совокупность методов, средств и мероприятий, используемых для обеспечения защиты.

В известных сейчас интегрированных средах и пакетах проектирования ТКС отсутствуют встроенные инструментальные средства для разработки подсистем обнаружения А-событий. Совокупность представленных в работе методов и технологий позволяет предложить структурно-функциональную схему инструментальных средств для реализации систем поддержки принятия решений по анализу и синтезу критериальных детекторов атак и решающих правил, которые могут быть использованы в качестве базисных при решении задач обнаружения А-событий в ТКС.

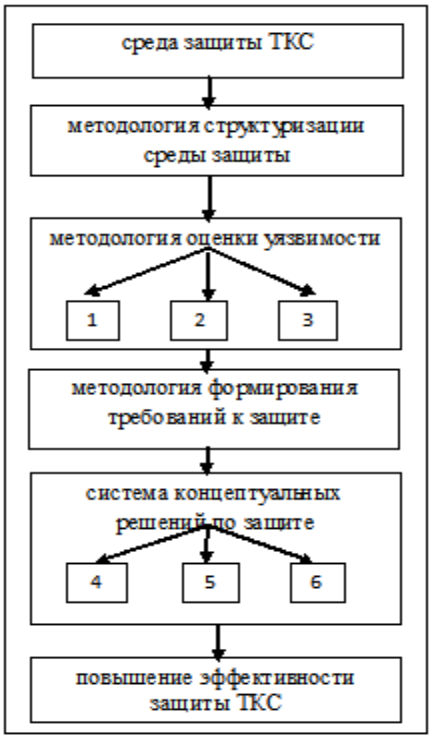

Рисунок 1 – Структурная схема концепции защиты ТКС:
1– система показателей уязвимости; 2 – система угроз безопасности информации;
3 – методы определения текущих и прогнозирования будущих значений показателей уязвимости;
4 – функции защиты; 5 – задачи защиты; 6 – средства защиты.

Структурно-функциональная схема СОВ представлена на рисунке 2.

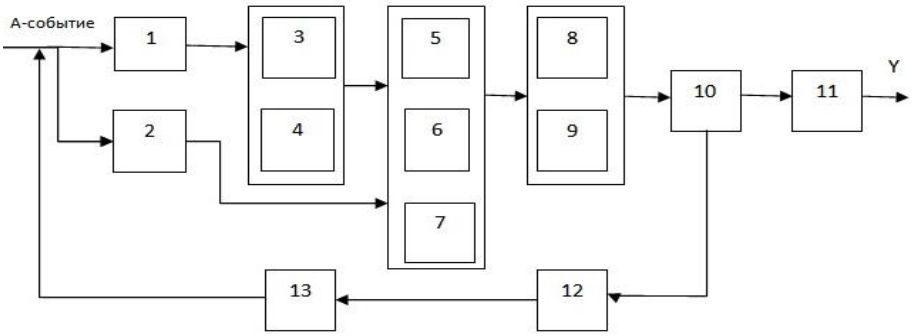

Рисунок 2 – Структурно-функциональная схема СОВ.

В состав СОВ входят следующие основные модули:

1 – выбор режима работы СОВ, 2 – задание параметров выборок, 3 – выбора модели интеллектуального анализа данных, 4 – выбора модели статистического анализа, 5 – обучения, 6 – тестирования, 7 – настройки, 8 – статистического анализа, 9 – адаптации, 10 – оценки достоверности результатов анализа, 11 – принятия решений об А-событии, 12 – принятия решений о модификации правил и параметров моделей, 13 – пополнения базы образцов сетевого трафика из сети интернет.

Использование системного подхода позволяет сформулировать основные принципы, которые положены в основу предлагаемой методологии разрабатываемой системы.

1. Предлагается использовать комплексный подход к обнаружению вирусных атак, который сочетает две дополняющие друг друга технологии. Первая позволяет предвосхищать будущие угрозы вирусных вторжений и базируется на методах интеллектуального анализа данных, в то время как вторая использует информацию об изменении вектора системных показателей ТКС.

2. Для реализации подходов требуется разработка структуры СОВ, которая содержит следующие функциональные модули: предварительной обработки; понижения размерности входных данных; настройки и тестирования, оптимизации настроечных параметров; классификации состояний сетевого трафика; адаптации параметров решающих правил к текущему состоянию трафика; поддержки принятия решений по формированию выходного сигнала о текущем состоянии трафика; определения достоверности контроля сетевого трафика в условиях дефицита априорной информации об источнике вторжений, включая определение ошибок первого и второго рода, объемы контролируемых выборок, моментов времени модификации решающих правил и др.

3. Функционирование СОВ должно поддерживаться ЛПР на основе многократных результатов измерений, получаемых при оценке значений контролируемых параметров нестационарного сетевого трафика за различные временные интервалы.

4. Тестирование системы должно быть не одноразовым, а постоянным в процессе функционирования СОВ, поскольку контролируемая среда является нестационарной и со временем информативность настраиваемых параметров решающих правил уменьшается.

5. Неизбежность использования средств имитационного моделирования, которое повышает быстродействие принятия решений при настройке параметров системы и восполняет дефицит контролируемой информации.

6. Концепция разработки СОВ должна иметь ограниченные возможности по ознакомлению с принципами ее построения. Это позволит уменьшить эффект от потенциальных угроз, которые могут быть осуществлены злоумышленниками.

7. 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.

8. Необходимо определить функции задачи исследования мощности статистических критериев, выделить структуру программного комплекса и связи между элементами структуры. Данные результаты необходимо использовать в дальнейшем для разработки и программирования исследовательского программного комплекса. При дальнейшем совершенствовании программного комплекса следует руководствоваться накопленным к этому моменту опытом его эксплуатации.

Выводы. На основе проведенного сравнительного анализа известных научных публикаций по теме предложена классификация подходов к построению детекторов и решающих правил обнаружения атак в телекоммуникационных сетях. Сформулированы перспективные направления исследований в области обнаружения атак в телекоммуникационных сетях с целью их своевременного обнаружения и принятия контрмер к их последствиям. ТКС, как одна из основных подсистем инфраструктур, должна обеспечивать высокую реактивность, достоверность и своевременность передачи информации между функциональными подсистемами инфраструктуры.

1. Решение задачи обеспечения информационной безопасности ТКС носит комплексный характер. В связи с этим авторами проведен функциональный и структурный анализ задачи обнаружения атак в телекоммуникационных сетях. В результате сформулированы методологические основы построения адаптивных систем интеллектуальной поддержки принятия решений по обнаружению несанкционированных вторжений в телекоммуникационных сетях.

2. Суть методологии сводится к использованию комплексного, системного подхода к обнаружению вирусных атак, который сочетает две дополняющие друг друга технологии. Первая позволяет предвосхищать угрозы вирусных вторжений на основе анализа функциональных характеристик объектов сети, в то время как вторая базируется на основе анализа состояния сетевого трафика. Такая СОВ должна поддерживаться ЛПР на основе многократных результатов измерений, получаемых при оценке значений контролируемых параметров нестационарного сетевого трафика за различные временные интервалы. Тестирование системы должно быть не одноразовым, а постоянным в процессе функционирования СОВ, поскольку контролируемая среда является стохастической и со временем информативность настраиваемых параметров решающих правил уменьшается.

3. На основе разработанных моделей созданы прототипы программных средств моделирования оценки эффективности системотехнических решений, полученных на основе предложенной методологии построения адаптивных интеллектуальных систем обнаружения вторжений.

Представлены результаты экспериментов по анализу эффективности информационной технологии критериального обнаружения атак и оценке уровня достоверности А-событий. Получены оценки ошибок первого и второго рода при классификации состояния трафика телекоммуникационной сети. Проведены эксперименты с целью исследования влияния на уровень правдоподобия различных объемов тестирующих выборок; адаптивного изменения значения метрик правил, а также различных значений весовых коэффициентов, которые задавались экспертом; были проведены специальные эксперименты для различных типов атак. Полученные результаты имеют статистически устойчивый характер и в целом презентативно отображают особенности предложенного подхода. Предложенные методы статистического моделирования и оценки вероятностей допущения ошибок первого и второго родов при обнаружении атак позволяют повысить обоснованность принимаемых решений с учетом рисков. Метод параметрической идентификации системных характеристик телекоммуникационной сети, отличается от известных использованием аналитических моделей многоэтапных процессов деградации и восстановления функциональных характеристик объектов сети.

4. Предлагаемая адаптивная модель обнаружения атак и возможных уязвимостей в компьютерных сетях на основе методов интеллектуального анализа данных может являться основой для IT-технологий обеспечения компьютерной безопасности в условиях адаптации при быстром изменении состояния сетевого трафика. Использование адаптивной модели системы принятия решений позволяет повысить уровень правдоподобия распознавания событий, минимизировать число ложных тревог, а также обеспечить высокую реактивность системы, что особенно важно для этапов раннего обнаружения.

Перспективы развития работ по теме связаны с широким использованием методов обеспечения компьютерной безопасности в современных информационных, распределенных, облачных технологиях, применяемых в различных областях человеческой деятельности.

Библиографический список использованной литературы

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

2. Kabiri P. Research in Intrusion Detection and Response. —A Survey/ P.Kabiri, A. Ghorbani. — International Journal of Network Security. — №:1, 2005. — P. 84–102.

3. Щеглов А. Ю. Защита компьютерной информации от несанкционированного доступа / А.Ю. Щеглов – М.:Наука и Техника, 2004г.– 384с.

4. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты / В.В. Домарев – М.:ТИД "ДС", 2002 г. – 688с.

Bryukhovetskyi A.A., Skatkov A.V., Voronin D.Y., Lovyagin V.S. Methodology of construction of intrusion detection system for computer networks.

Presents a comprehensive approach to building Intrusion Detection System, which combines two complementary technologies. The first allows you to recognize the threat of network intrusion and is based on data mining techniques, while the second uses the information on changes in the vector system performance computer network.

Key words: detection of network attacks, information security critical systems.

УДК 004.75

К.С. Ткаченко
Севастопольский национальный технический университет
ул. Университетская 33, г. Севастополь, Россия, 299053
e-mail: tkachenkokirillstanislavovich@mail.ru, tkachenkokirillstanislavovich@gmail.com

АЛГОРИТМ ДОМИНИРУЮЩЕГО ВЫБОРА ВАРИАНТОВ ДЛЯ ПРИНЯТИЯ РЕШЕНИЙ В УСЛОВИЯХ ВИРУСНОЙ АТАКИ

Предлагается алгоритм стохастической аппроксимации с выбором доминирующего варианта. Приводятся результаты вычислительного эксперимента.

Ключевые слова: *стохастическая аппроксимация.*

Как известно [1 — 4], необходимыми составляющими любых современных сложных систем являются средства адаптивного выбора вариантов, в том числе и для динамической реконфигурации в условиях вирусной атаки. Перспективными алгоритмами для решения задач адаптивного выбора в условиях априорной неопределенности входных данных являются рекуррентные алгоритмы, предназначенные для решения задач безусловной минимизации [1]. Поэтому задача разработки нового