УДК 519:616-079.4:616.5

АНАЛИЗ ПОДХОДОВ К ПРАКТИЧЕСКОЙ РЕАЛИЗАЦИИ СИТУАЦИОННЫХ АЛГОРИТМОВ ОБНАРУЖЕНИЯ СЕТЕВЫХ АНОМАЛИЙ

В.С. СИМАНКОВ, А.С. КОЛОДИЙ

Применяемые в настоящий момент методы обнаружения аномалий (методы сигнатурного анализа, ситуационного подхода, статистического анализа, искусственных нейронных сетей и др.) на сегодняшний день используются в существующих реализациях систем обнаружения, однако не обладают возможностью анализа всех необходимых данных. В рамках одного комплекса целесообразно внедрение архитектуры, допускающей совместное применение различных методов для использования единых систем аудита и улучшения свойств адаптивности с учетом типовых сценариев развития аномалии.

Ключевые слова: сетевые аномалии, ситуационное моделирование, выявление аномалий, сигнатурный анализ.

На сегодняшний день можно выделить два основных подхода к обнаружению сетевых аномалий («anomaly detection»). Первый подход полагается на модель аномалий (аномального поведения) и сравнивает поток событий в системе с некоторыми моделями. Подход, связанный с обнаружением аномального поведения, полагается на модель нормального поведения и идентифицирует аномальные вхождения в поток событий (отклонения от нормального поведения) [5].

Для систем обнаружения атак характерно наличие ошибок 1-го и 2-го рода: ошибка первого рода состоит в том, что будет отвергнута правильная гипотеза (будет пропущено состояние, которое не попадает под определение аномального поведения или шаблон — «false negative»); ошибка второго рода состоит в том, что будет принята неправильная гипотеза (нормальные действия в работе системы будут расценены как аномалия — «false positive»).

Авторами были рассмотрены некоторые применяемые в настоящий момент методы обнаружения аномалий на уровне сети и узлов сети: методы сигнатурного анализа, ситуационного подхода и методы статистического анализа. Отдельно стоит указать методы на основе искусственных нейронных сетей; искусственные иммунные системы, биометрические методы, методы кластерного анализа, экспертные системы.

Некоторые из этих методов на сегодняшний день используются в существующих программных и аппаратно-программных реализациях систем обнаружения: система обнаружения Snort, система Bro, комплекс программных средств STAT, Prelude, OSSEC, аппаратно-программные средства Cisco Secure IPS, система IBM ISS RealSecure, средства Symantec Network Security, eTrust Intrusion Detection.

Однако ни одна из рассмотренных СОА не обладает возможностью анализа всех необходимых данных, обрабатываемых на разных уровнях информационных систем.

Анализ существующих методов показал, что в рамках одной СОА целесообразно внедрение архитектуры системы, допускающей совместное применение различных методов для решения задач защиты сетей, а также для улучшения свойств адаптивности сигнатурных методов требуется алгоритм поиска неточного соответствия искомым шаблонам, удовлетворяющий следующим критериям [2]:

– высокая ожидаемая скорость работы;

– возможность эффективной программной реализации;

– возможность обобщения алгоритма на поиск с неточным соответствием искомому образцу.

Модели сетевой аномалии разрабатываются для решения следующих задач: обеспечения единого представления сведений о регистрируемых событиях в рамках одной модели, для обработки данных, поступающих с различных подсистем ИС, и уменьшения количества ложных срабатываний.

Уменьшение числа ложных срабатываний должно достигаться за счет учета для каждого события фазы сетевой аномалии, к которой оно может относиться, и корреляционных связей событий в наблюдаемой последовательности. Таким образом, предлагаемая модель призвана учитывать типовой сценарий развития сетевой аномалии в компьютерной системе.

Каждое событие безопасности описывается рядом характеристик, таких, как: тип события, время регистрации, фаза аномалии, в которой может наблюдаться данное событие, источник, цель. Источники могут описывать сетевой узел с набором адресов, процессы, системные службы, пользователей, имена файлов, имена ключей системного реестра [3].

Важными свойствами в описании каждого события являются:

– фаза, в которой может наблюдаться данное событие;

– время появления события;

– базовая оценка опасности события;

– время ожидания, в течение которого оценка остается актуальной.

Для практической реализации такого модельного подхода необходимо предъявлять дополнительные требования к архитектуре сенсоров системы, сделать ее модульной (рис. 1). Сенсор СОА, построенный по модульному принципу, имеет ряд преимуществ перед «монолитным»:

– возможность обработки первичных данных произвольной природы: сетевой трафик, системные вызовы, файлы журналов, контроль прикладных средств;

– возможность, при необходимости, использования произвольных методов обнаружения злоупотреблений или аномалий;

– возможность адаптивной настройки под конкретную сеть путем включения или исключения требуемых модулей из рабочего множества сетевого сенсора.

Рис. 1. Общая структура предлагаемой модели СОА

Под управлением ядра операционной системы работает некоторое количество процессов, потенциально уязвимых к вторжениям. При обращении к ресурсам системы от процессов к ядру поступают системные вызовы, которые перехватываются модулем аудита. Перехваченные последовательности поступают на вход модуля обнаружения для анализа на предмет наличия аномалий. Модуль обнаружения сравнивает данные, поступающие от модуля аудита, с соответствующим профилем, хранящимся в базе данных моделей [4-6]. При обнаружении аномалии в текущей последовательности системных вызовов он записывает сообщение об этом в журнал событий и оповещает об этом модуль реагирования, который, в соответствии с настройками политики реагирования, оказывает воздействие на исполняемый процесс, например, снимает его с выполнения.

Функционирование системы включает два этапа: обучение и обнаружение. Целью этапа обучения является сбор в базе данных примеров максимально полной и в то же время компактной информации о нормальном поведении процесса и настройка модели процесса таким образом, чтобы она максимально достоверно моделировала это поведение [1]. В режиме обнаружения анализируются последовательности системных вызовов, также собранные модулем аудита, но, возможно, содержащие аномальные участки. Происходит сопоставление фрагментов последовательностей, характеризующих профиль нормального поведения рассматриваемого процесса, и генерируются сигналы тревоги, если при сопоставлении возникли существенные отклонения от профиля.

Наиболее обоснованным решением для реализации сбора исходной информации в разрабатываемой системе является специализированный модуль ядра, осуществляющий перехват системных вызовов. Из известных решений можно использовать BSM для ОС Solaris или LinuxBSM для ОС семейства GNU/Linux.

На современном этапе развития СОА методы обнаружения аномалий не находят практического применения в чистом виде, а используются как дополнения к методам обнаружения злоупотреблений, расширяющие функциональность СОА

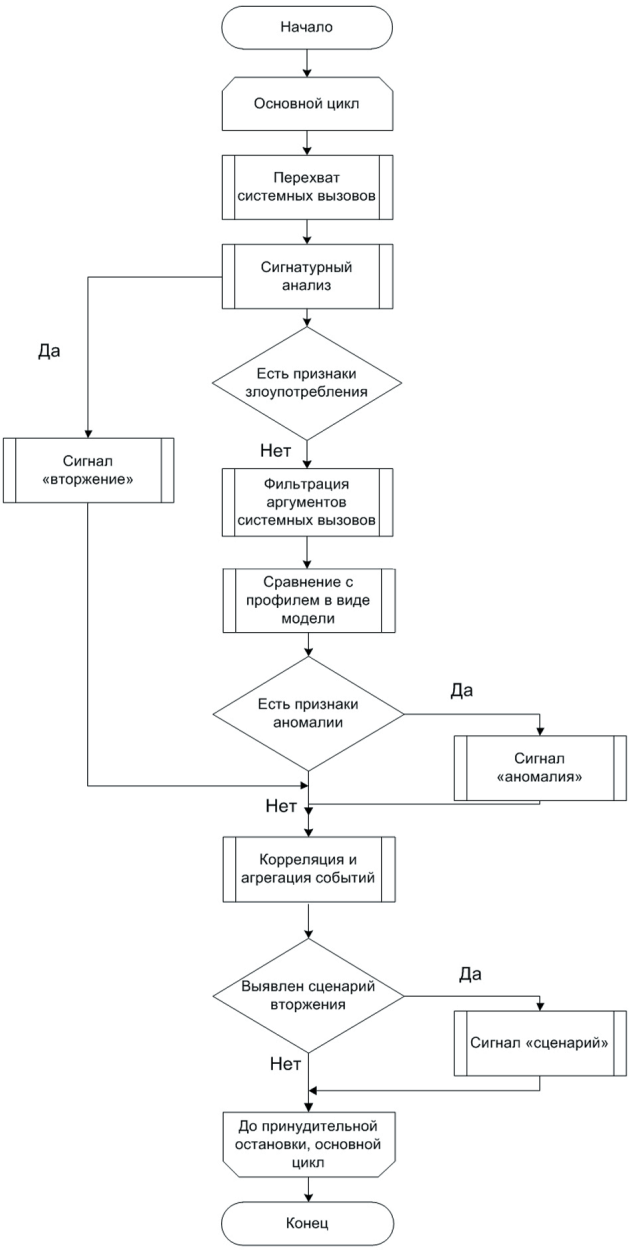

Рис. 2. Общий алгоритм функционирования комплексной СОА

в целом [3]. Рассмотрим возможность применения разработанного метода обнаружения аномалий в возможной структуре комплексной СОА. Разработанный метод обнаружения аномалий предполагает анализ данных аудита, представляющих собой последовательности системных вызовов, поступающих к ядру от системных и прикладных процессов. При этом анализируются только сами вызовы без их аргументов. Разработанный метод обнаружения можно использовать в комплексе с произвольной системой обнаружения уровня узла, анализирующей системные вызовы.

Учитывая изложенные соображения, сформулируем общий алгоритм функционирования комплексной СОА (рис. 2).

Такая комплексная СОА может использовать единую систему аудита, причем на вход модуля обнаружения злоупотреблений целесообразно подавать весь объем поступающих данных, а на вход модуля обнаружения аномалий системные вызовы без учета их аргументов. При использовании в рамках комплексной СОА модулей обнаружения аномалий и модуля обнаружения злоупотреблений возникает необходимость агрегации сообщений от этих двух источников, анализа динамики и выявления типовых сценариев вторжений [4].

Агрегация и корреляция событий необходимы для устранения традиционных недостатков обнаружения злоупотреблений и обнаружения аномалий.

Программная система обнаружения состоит из (рис. 3):

– сетевых сенсоров, объединяющих модули, предназначенные для анализа событий, представляющих интерес с точки зрения безопасности контролируемой сети и ее узлов;

– аккумулятора событий безопасности, предназначенного для приема, хранения и централизованного анализа всех событий безопасности, а также для управления сетью сенсоров в автоматическом режиме;

– консоли управления для управления системой и визуализации данных.

Для возможности проведения экспериментальных исследований были реализованы в реальной распределенной сети (рис. 4) обработчики сенсора, обеспечивающие: декодирование сетевых кадров ethernet, пакетов PPPoE, ARP, IPv4, обработчики выполняющие дефрагментацию IP пакетов и сборку сеансов TCP, модули обнаружения сетевых атак ARP-spoofing, модули выявления атак типа syn-flood, fragle, smurf и некоторых видов сетевого сканирования, модуль выполнения сигнатурного поиска с неточным соответствием, модули анализа файловой системы и журналов регистрации операционной системы.

Экспериментальные исследования проводились с целью:

– проверки работоспособности предложенных решений по обработке сетевого трафика

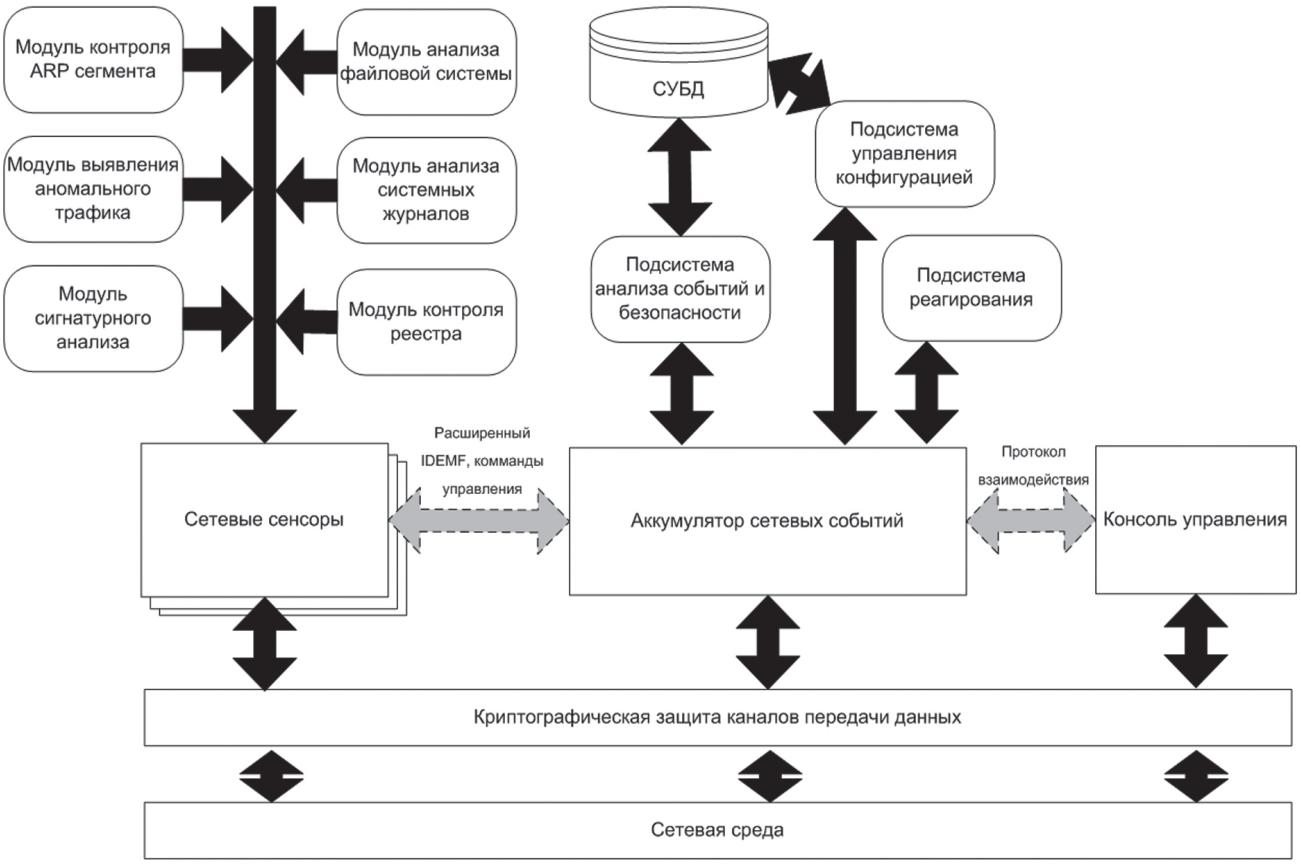

Рис. 3. Архитектура программной системы обнаружения атак

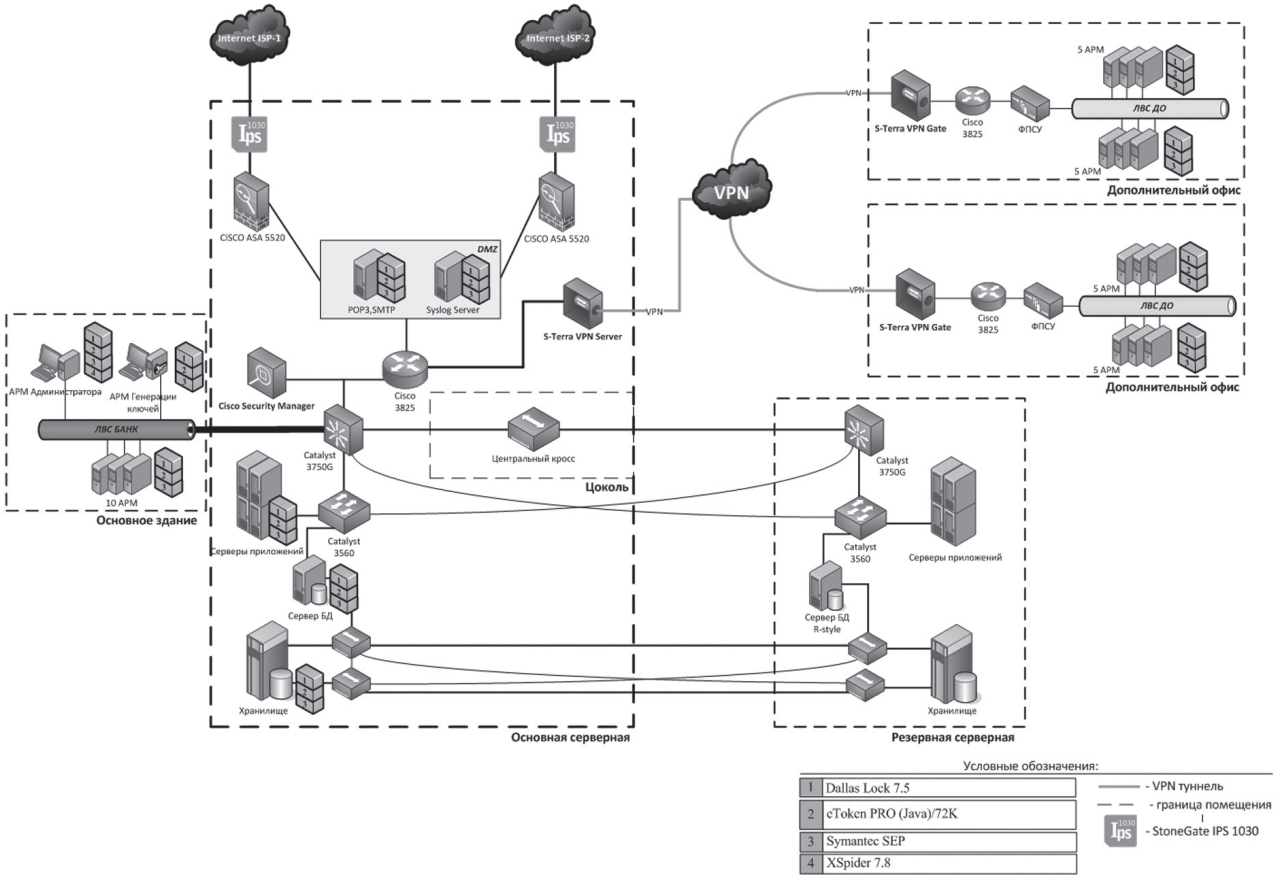

Рис. 4. Схема тестовой сети

и локальных событий, в том числе способности анализировать пакеты канального, сетевого уровня, производить сборку TCP-сессий;

– оценки временных характеристик выполнения автоматизированных функций, реализуемых с применением макета программной системы;

– сравнения результатов, получаемых разработанной программной системой с результатами существующих СОА.

По результатам испытаний на производительность с различными наборами обработчиков и количеством сигнатур макет показал возможность обработки трафика со скоростью 10.6 Мб/с (7500 сигнатур на ЭВМ с центральным процессором Intel Core i3, 4 Гб ОЗУ), что достаточно для обработки каналов со скоростью 100 Мбит/с.

Литература

[1] *Симанков В.С., Шпехт И.А.* Автоматизация системных исследований на основе неформальных процедур: Монография. – М.: БиномПресс, 2012. – 358 с.

[2] *Раттнер. Д.* «Анализ рисков в управлении сетевой безопасностью.». — Northeastern University, 2010.

[3] *Дымарский Я.С., Крутякова Н.П., Яновский Г.Г.* Управление сетями связи: принципы, протоколы, прикладные задачи. — Москва, 2010.

[4] *Abraham A. and Thomas J.,* Distributed Intrusion Detection Systems: A Computational Intelligence Approach. // Applications of Information Systems to Homeland Security and Defense, Abbass H.A. and Essam D. (Eds.), Idea Group Inc. Publishers, USA, 2005.

[5] *Blanc M., Oudot L., and Glaume V.,* «Global Intrusion Detection: Prelude Hybrid IDS.» // Technical Report, 2003.

[6] *Noria Foukia,* "IDReAM: Intrusion Detection and Response executed with Agent Mobility Architecture and Implementation."// Proceedings of the fourth international joint conference on Autonomous agents and multiagent systems, the Netherlands, 2005.

Поступила в редколлегию 15.05.2012

Симанков Владимир Сергеевич, доктор технических наук, профессор, директор Института информационных технологий и безопасности университетского комплекса Кубанского государственного технологического университета, г. Краснодар. Область научных интересов: системный анализ, синтез, моделирование, оптимизация, адаптивное управление.

Колодий Александр Сергеевич, аспирант кафедры компьютерных технологий и информационной безопасности Кубанского государственного технологического университета, г. Краснодар. Область научных интересов: системный анализ, моделирование, информационная безопасность, сети передачи данных.

УДК 519:616-079.4:616.5

Аналіз підходів до практичної реалізації ситуаційних алгоритмів виявлення мережевих аномалій / В.С. Сіманков, О.С. Колодій // Прикладна радіоелектроніка: наук.-техн. журнал. – 2012. – Том 11. № 3. – С. 421–425.

Застосовувані в даний момент методи виявлення аномалій (методи сигнатурного аналізу, ситуаційного підходу, статистичного аналізу, штучних нейронних мереж і ін) на сьогоднішній день використовуються в існуючих реалізаціях систем виявлення, однак не володіють можливістю аналізу всіх необхідних даних. В рамках одного комплексу доцільно впровадження архітектури, що допускає спільне застосування різних методів для використання єдиних систем аудиту і поліпшення властивостей адаптивності з урахуванням типових сценаріїв розвитку аномалії.

Ключові слова: мережеві аномалії, ситуаційне моделювання, виявлення аномалій, сигнатурний аналіз.

Іл. 04. Бібліогр.: 06 найм.

UDC 519:616-079.4:616.5

Analyzing approaches to practical realization of situational algorithms of detecting network anomalies / V.S. Simankov, A.S. Kolodiy // Applied Radio Electronics: Sci. Journ. – 2012. Vol. 11. № 3. – P. 421–425.

Currently used methods of detecting anomalies (methods of signature analysis, situational approach, artificial neural networks, etc.) are applied in existing realizations of detection systems, however they do not have a possibility of analyzing all the necessary data. Within one complex it is expedient to introduce an architecture allowing a joint application of various methods for using unified audit systems and improving adaptive features in view of standard scenarios of anomaly development.

Keywords: network anomalies, situational modelling, detection of anomalies, signature analysis.

Fig. 04. Ref.: 06 items.