КЛАССИФИКАЦИЯ МЕТОДОВ ОБНАРУЖЕНИЯ АТАК

CLASSIFICATION OF ATTACK DETECTION METHODS

УДК 004.056.53

Комаров А.Н., магистрант Донской государственный технический университет Россия, г. Ростов-на-Дону

Komarov A. N., barytonalex@gmail.com

Аннотация

В статье рассматривается основополагающие методы обнаружения сетевых атак. Также в статье уделяется внимание построению обобщенной схемы классификации методов обнаружения сетевых атак, а именно предложен вариант формирования данной классификации. Проведен анализ эффективности использования методов обнаружения сетевых атак, рассматриваемых в данной работе. Предложен наиболее перспективный вариант развития систем обнаружения сетевых атак, основанный на гибридизации подходов и увеличении производительности таких систем.

Summary

The article discusses the fundamental methods of detecting network attacks. The article also pays attention to the construction of a generalized classification scheme for methods of detecting network attacks, namely, a variant of the formation of this classification is proposed. The analysis of the effectiveness of the use of methods for detecting network attacks, considered in this paper. The most promising variant of the development of network attack detection systems based on hybridization of approaches and an increase in the performance of such systems is proposed.

Ключевые слова: аномалии, сетевой трафик, алгоритм, атака, информация.

Key words: anomalies, network traffic, algorithm, attack, information.

Классификация систем обнаружения атак по способам выявления атак включает в себя системы обнаружения аномалий и системы обнаружения злоупотреблений. На рисунке 1 показана схема обнаружения сетевых аномалий на основе показателей сетевого трафика.

Алгоритм обнаружения сетевых аномалий описывается следующим образом. Данные для анализа представляют собой сетевой трафик в виде набора сетевых пакетов, в общем случае фрагментированных на уровне IP. Следующим шагом является сбор данных без их обработки, такие данные послужат источником при формировании информационной базы для последующего анализа. Данная информационная база может быть агрегирована за определенный интервал времени и нормализованы с целью задания признаковых атрибутов общего вида, такие данные понадобятся при создании текущего профиля активности. Текущий профиль активности сравнивается с шаблоном нормальной деятельности объекта. При обнаружении существенных расхождений сравниваемых параметров профиля, фиксируется сетевая аномалия. Иначе происходит уточнение сохраненного шаблона нормального поведения путем корректировки показателей с учетом текущей ситуации при проверке сетевой активности.

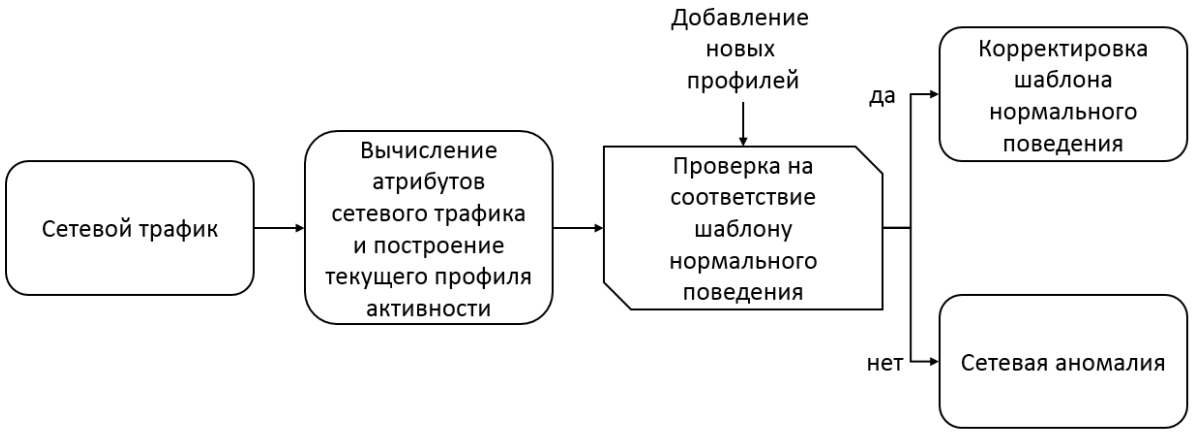

Рисунок 1 – Схема обнаружения сетевых аномалий

Описанный алгоритм имеет несколько вариантов для реализации подсистемы контроля на соответствие шаблону нормальной деятельности объекта. Наиболее простейшим вариантом является процедура сравнения с

предельной величиной, когда собранные результаты, показывающие текущее состояние сетевой активности, подлежат сравнению с экспертно задачной числовой планкой. При выявлении превышений предельной величины, фиксируется сетевая аномалия.

Описание шаблона нормального поведения является не тривиальной задачей, и зачастую не всегда имеет однозначного решения. На практике же оказывается, что не каждое аномальное поведение есть атака [1]. Например, при отладочных действиях администратора сети, использующего такие утилиты как ping, mtr, traceroute при диагностики сетевого трафика, системой будут определены как аномальная сетевая активность, хотя на самом деле не преследуют никаких нелегальных действий.

Далее рассмотрим схему обнаружения злоупотреблений [2] в сетевом трафике, которая показана на рисунке 2.

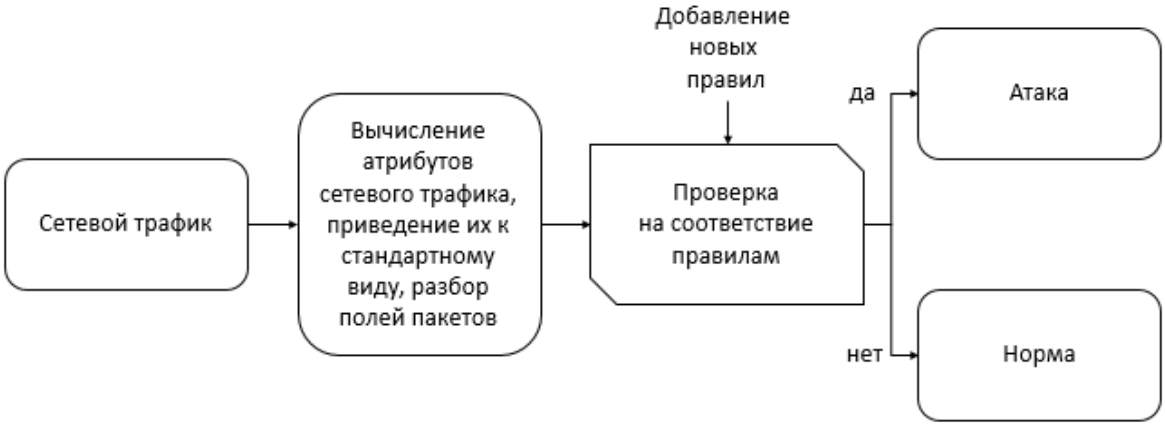

Рисунок 2 – Схема обнаружения злоупотреблений в сети

Метод обнаружения злоупотреблений основан на идентификации несанкционированных действий, если имеется точное представление в виде шаблонов атак. Шаблон атак представляет собой совокупность действий, описывающих конкретную атаку, применив которые к показателям объекта можно точно определить принадлежность к данной атаке. Первичными данными также, как и для схемы обнаружения сетевых аномалий является сетевой трафик.

При создании любой системы обнаружения злоупотреблений ключевой проблемой является вопрос эффективного проектирования механизма задания правил. Формирование исчерпывающей базы правил для возможности определить всевозможные атаки является невозможным в виду некоторых

факторов. Так как описание различных вариантов атакующих действий негативно влияют на производительность системы. А при незначительных изменениях в действиях атакующего приводят к невозможности распознать такого рода атаку, то задаваемые правила должны быть универсальны, чтобы покрыть как можно большее число известных видов сетевых атак.

Можно сделать вывод что использование метода обнаружения злоупотреблений применимо только для известных типов атак, а для обнаружения неизвестных атак является безуспешным.

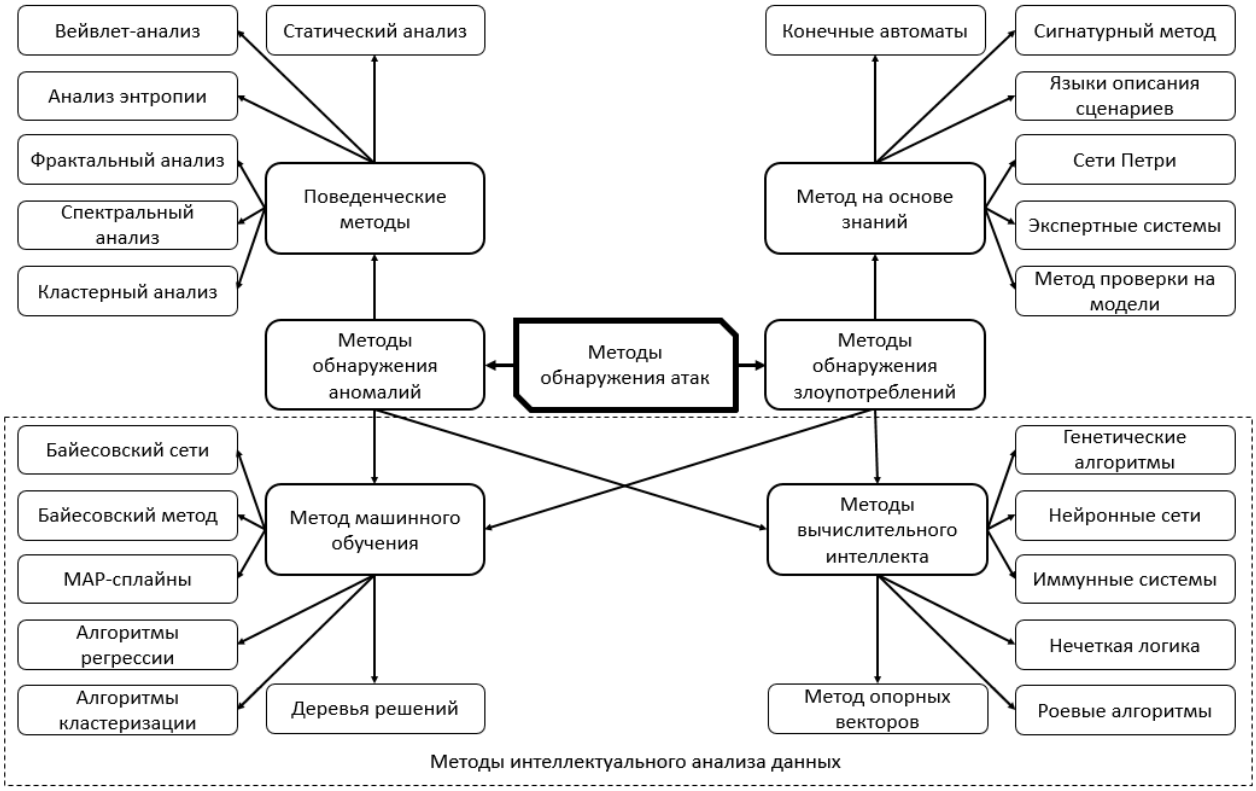

Рисунок 3 – Классификация методов обнаружения атак

Классификация методов обнаружения атак, показанная на рисунке 3, является условной и не претендует на полноту, некоторые подходы на схеме могут относится к нескольким группам.

В данной классификации выбрано такое разбиение, при котором методы интеллектуального анализа данных классифицируются по критерию их принадлежности к биоподобным алгоритмам и поэтому содержат в себе два класса:

– методы вычислительного интеллекта;
– методы машинного обучения.

В статье приведен анализ методов обнаружения сетевых атак. Рассмотренные методы успешно применяются при разработке новых систем обнаружения атак. Предложена классификация рассмотренных методов. Предложены варианты по использованию методов интеллектуального анализа информации в системах обнаружения сетевых аномалий.

Перспективным направлением развития систем обнаружения атак заключается в применении гибридизации подходов, которые позволили бы пользоваться всеми преимуществами сигнатурных и эвристических методов, а также использование проактивного мониторинга безопасности. Одним из основных требований, предъявляемых к данным решениям, является обеспечение адаптивной и высоко масштабируемой аналитической обработки событий, позволяющей обеспечить интеллектуальное управление большим объемом данных о безопасности в реальном времени.

Использованные источники

1. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей //М.: ИД «ФОРУМ»: ИНФРА-М. 2008. 416 с.
2. Ghorbani A.A., Lu W., Tavallaee M. Network Intrusion Detection and Prevention: Concepts and Techniques // Springer Science & Business Media. 2009. 212 p.

Sources used

1. Shang'in V. F. Information security of computer systems and networks / / Moscow: ID "FORUM": INFRA-M. 2008. 416 p.
2. Ghorbani A. A., Lu W., Tavallaee M. detection and prevention of network intrusions: concepts and methods / / Springer Science & Business Media. 2009. 212 p.