УДК 004.56

Аброськина Е.С.

Студент-магистр

2 курс, факультет «Отдел магистратуры»

Поволжский государственный университет телекоммуникаций и информатики

Самара, Россия

АНАЛИЗ МЕТОДОВ ВЫЯВЛЕНИЯ СЕТЕВЫХ ВТОРЖЕНИЙ И АНОМАЛИЙ

Аннотация: *Данная статья посвящена анализу различных методов выявления сетевых вторжений и аномалий. Производится полный анализ самых известных методов для обнаружения и классификация сетевых атак и аномалий, выведена более обобщенная схема классификации данных методов. Проводится более подробный разбор групп методов таких как поведенческие, методы машинного обучения, вычислительного интеллекта, а также методов на основе знаний.*

Ключевые слова: *метод, защита информации, угроза, компьютерная сеть, ПО, атака, аномалия, нейронная сеть, информационная безопасность.*

Abroskina E.S.

Student-magistr

2nd year, faculty "Department of magistracy"

Volga State University of Telecommunications and Informatics

Samara, Russia

ANALYSIS OF METHODS FOR DETECTING NETWORK INTRUSION AND ANOMALIES

Annotation: *This article is devoted to the analysis of various methods for detecting network intrusions and anomalies. A full analysis of the most famous methods for detecting and classifying network attacks and anomalies is carried out, a more generalized classification scheme for these methods is derived. A more detailed analysis of groups of methods such as behavioral, machine*

learning, computational intelligence, and knowledge-based methods is carried out.

Key words: *method, information protection, threat, computer network, software, attack, anomaly, neural network, information security.*

Стремительное развитие в сфере IT-технологий в настоящее время порождает множество вопросов связанных с безопасностью данных и сетевых ресурсов. В современном мире, вопросы касаемые обнаружения атак и различных аномалий в сети остаются актуальными, также создается множество методов и решений борьбы с ними. Существует множество работ, которые посвящены данной теме, однако не многие охватывают большой круг проблем, т.к. были сделаны довольно давно и некоторых проблем, затронутые в данной статье, не было выявлено на тот момент. В настоящей статье будет подробно рассмотрена классификация методов обнаружения атак, их преимущества и недостатки.

По способу выявления атак средства обнаружения подразделяются на:

- Системы обнаружения аномалий;
- Системы обнаружения злоупотреблений.

На рисунке 1 представлена схема обнаружения аномалий на основе показателей сетевого трафика.

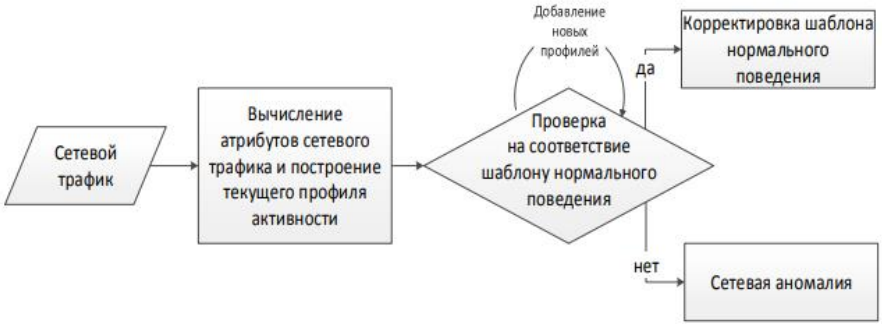

Рис.1 Схема обнаружения аномалий

На рисунке 2 представлена схема обнаружения злоупотреблений в сетевом трафике. Обнаружение злоупотреблений позволяет выявлять неправомерные действия, если имеется их точное представление в виде шаблонов атак. В данном случае под шаблоном атаки подразумевается некоторая совокупность, которая явно описывает атаку действий, которые применяя к определенному объекту можно получить однозначный ответ о его принадлежности к этой атаке.

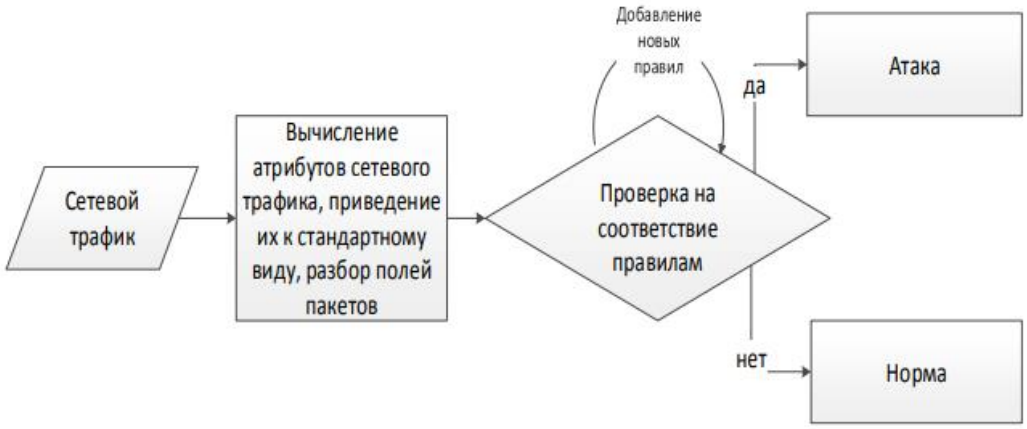

Рис.2 Схема обнаружения злоупотреблений

Для построения полной схемы классификации методов выявления сетевых атак, отталкиваясь от двух главных систем обнаружения, был выполнен анализ огромного списка работ (рис. 3). Рассмотрим каждую группу методов подробнее.

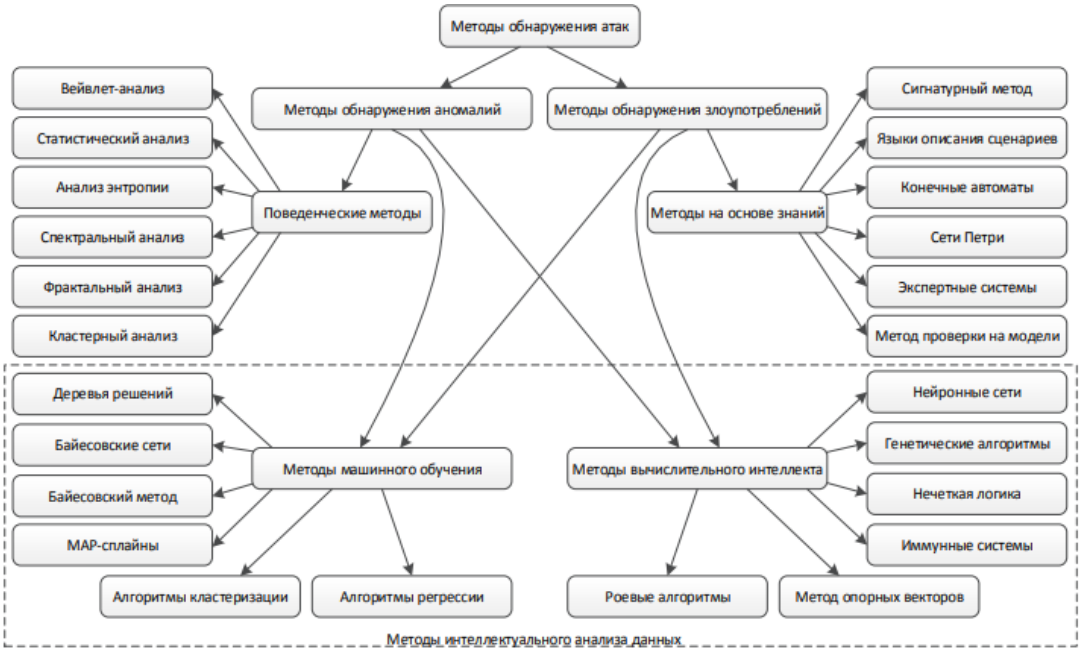

Рис. 3 Классификация методов обнаружения сетевых атак

Поведенческие методы. Поведенческими методами называются методы, которые на основе статистических моделей определяют показатели, характеризующие параметры штатного поведения системы.

Преимущества:

- Позволяют определять распределенные атаки, в том числе и распределенные во времени;
- Определяют взаимосвязи между различными событиями;

- Корреляция событий позволяет определить значимые события.

Недостатки:

- чувствительность зависит от заданной величины отклонений и от точности модели информационной системы.

Данные методы обнаружения атак определяются наличием ложноположительных срабатываний, объясняющиеся сложностью полного и точного описания большого количества правомерных действий пользователями. Также для многих аналогичных систем нужно проведение этапа предварительной настройки. Длительность интервала сбора данных может занимать несколько недель или даже несколько месяцев.

К поведенческим методам относятся:

- вейвлет-анализ;
- анализ энтропии;
- фрактальный анализ;
- статистический анализ;
- спектральный анализ;
- кластерный анализ.

Вейвлет-анализ заключается в построении коэффициентов, которые используются в разложении исходного сигнала по базисным функциям. В качестве сигнала может выступать интенсивность сетевого трафика или данные о корреляции IP-адресов назначения. Выполнение данного метода позволяет выявить наиболее важную информацию как сигнал, который соответствует колебаниям с высокой амплитудой, и игнорировать менее полезную информацию в колебаниях с низкой амплитудой как шумовую составляющую.

Анализ энтропии применяется при обнаружении атак для формирования статистического критерия с целью проверки принадлежности исследуемого экземпляра аномальному классу.

Энтропия множества x определяется:

$$H(x) = -\sum_{x \in X} P(x)\, log_2\, P(x),$$

где P(x) обозначает вероятность появления элемента x в множестве X.

Суть данного метода в том, чтобы при построении модели максимизировать значении энтропии. Это нужно, чтобы стало верным предположение, что с увеличением числа уникальных записей происходит их равномерное распределение относительно выбранных классов множества X, что приводит к увеличению энтропии.

Фрактальный анализ основан на том, что сетевой трафик удовлетворяет свойству самоподобия, важными понятиями в котором являются параметр Херста H и фрактальная хаусдорфова размерность D:

$$H = log_{N/2}\frac{R}{s},$$
$$D = 2 - H,$$

где N – длина временного ряда $X = \{x_1, \ldots, x_n\}$ со средним значением $\bar{x} = \frac{1}{N}\sum_{i=1}^{N} x_i$, $R = \max_{1\le i\le N} x_i - \min_{1\le j\le N} x_j$ – размах отклонения (изменчивость) ряда, $s = \sqrt{\frac{1}{N-1}\sum_{i=1}^{N}(x_i - \bar{x})^2}$ – выборочное среднеквадратическое отклонение. Для самоподобных процессов выполняется соотношение $0.5 < H < 1$. На малых временных отрезках аномальный и нормальный трафики характеризуются различными значениями показателя Херста.

Статистический анализ является основой методов обнаружения аномалий в сети. К данной группе относятся:

- цепи Маркова;
- метод хи-квадрат;
- пороговый анализ;
- анализ временных рядов;
- метод среднеквадратичных отклонений;
- метод распределения интенсивности передачи/приема пакетов.

Важно, что в статистических системах главную роль играет верный выбор контролируемых параметров, которые характеризуют отличия в нормальном и аномальном трафиках. Достоинствами статистических методов является их адаптивность к изменению поведения пользователя, а также способность к обнаружению модификаций атаки. Недостатками являются высокая вероятность возникновения ложных сообщений об атаках и зависимость от порядка следования событий.

Спектральный анализ является частным случаем вейвлет-преобразования, позволяющий выделять наиболее информативные составляющие исследуемого процесса с помощью изменения размерности исходного пространства признаков.

В основу данного подхода легло предположение, что полученные компоненты аномального трафика отличаются от компонентов обычного трафика. Главные компоненты выбираются таким образом, чтобы они соответствовали наибольшей изменчивости исходного процесса. Остальные компонент рассматриваются как составляющие шума.

Суть кластерного анализа заключается в выделении таких характеристик из сетевого трафика, которые позволят разбить классифицируемые объекты (пакеты, соединения) на группы, соответствующие нормальному функционированию сетевого взаимодействия. Все остальные экземпляры, которые не попадают в построенные области, классифицируются как аномальные.

Методы на основе знаний. К методам, в основе которых лежат знания, относят методы, в контексте которых заданы факты, правила вывода и сопоставления, которые отражают признаки определенных атак и применяются для обнаружения атак на основе заложенного механизма поиска. В качестве процедур поиска может применяться сравнение по шаблону, анализ перехода состояний, аппарат регулярных выражений и т.д. Данные методы применяются в работе с базой знаний, в которую включены описания уже известных атак.

В сигнатурных методах системные события представлены в виде цепочек символов из некоторого алфавита. Суть данных методов состоит в задании множества сигнатур атак в виде регулярных выражений или правил на основе сравнения с образцом и проверке соответствия наблюдаемых событий данным выражениям. Примерами данных методов выступают Snort и Suricata.

Преимущества сигнатурных методов в том, что обнаружение известных атак осуществляется очень эффективно. Однако, применение базы сигнатур большого объема негативно влияет на работоспособность системы обнаружения.

Метод на основе конечных автоматов моделирует атаки в виде взаимосвязанной сети из состояний и переходов. Атака считается успешной, если последовательность действий атакующего приводит систему в нестабильное состояние. Каждое состояние можно представить как слепок характеристик безопасности, переходы между ними соответствуют успешному выполнению события , приводящее систему в совершено новое состояние. К нескольким экземплярам конечного автомата относится практически каждое наблюдаемое событие, представляющие собой определенный сценарий атаки.

Еще одним примером обнаружения злоупотреблений на основе анализа переходов состояний является IDIOT (Intrusion Detection In Our Time), применяющий метод раскрашенных сетей Петри. Сценарии вторжений кодируются в шаблоны IDIOT, и события безопасности проверяются путем их сравнения с данными шаблонами. Достоинством этого метода является возможность визуального представления атаки в виде диаграмм перехода состояний, а также в способности системы

выявить атаку до ее фактического совершения. Недостаток – сложность реализации.

В основу функций экспертных систем легло применение правил вывода к данным о входных событиях. Они представлены в виде систем, которые принимают решения о принадлежности события к определенному классу атак на основании заданных правил.

Преимуществами данного метода являются возможность выделения управляющей части правила от части, которая задает решение, высокая скорость работы и возможность обеспечения отсутствия ложных тревог. Недостатками – невозможно обнаружить неизвестные атаки, зависимость системы от ее полноты, корректности и актуальности правил, которые заложены в базу знаний, снижение эффективности работы с увеличением объема данных.

Методы машинного обучения. Данные методы используются не только для обнаружения аномалий в сети, но и для обнаружения злоупотреблений. Это обусловлено тем, что указанные подходы в качестве исходных данных для обучения чаще всего используют образцы как нормального, так и аномального поведения в сети.

Наиболее часто используемым методом обнаружения атак является байесовская сеть. Байесовская сеть – модель, кодирующая вероятностные отношения между рассматриваемыми переменными и Байесовская сеть – это модель, кодирующая вероятностные отношения между рассматриваемыми переменными и предлагает некоторый механизм для вычисления условных вероятностей их наступления. Частным случаем данной модели является байесовский классификатор. Он позволяет оценить апостериорную вероятность принадлежности экземпляра заданному классу на основе безусловной теоремы Байеса.

Для определения априорных и апостериорных вероятностей новых атак используют псевдобайесовкие оценочные функции. Справедливо также утверждение, что вследствие свойств предложенного метода системе не нужны предварительные знания об образцах новых атак.

Интеллектуальный модуль применяет правила ассоциации $X \rightarrow Y$ к записям соединений, где X и Y соответственно предусловие и постусловие правил, описанных внутри ядра системы. Этот модуль работает в двух режимах:

- Режим обучения - режиме происходит построение профилей нормального поведения пользователей и системы, и генерируются правила ассоциации, которые будут использоваться для обучения модуля классификации;

- Режим обнаружения - режиме интеллектуальный модуль получает ранее не встречавшиеся правила ассоциации, которые отличаются от профиля.

Данный модуль предусматривает три уровня работы:

- Обособленный уровень – имеет два режима: статический (используется во время нормальной работы системы, когда создается профиль для поведения системы) и динамический анализ (использует метод скользящего окна для поэтапного анализа правил ассоциации);
- Уровень домена – система отслеживает IP-адреса отправителя и получателя. Соединение считается подозрительным, если эти адреса принадлежат одной и той же подсети;
- Уровень выборки признаков - система собирает слепки сетевого поведения каждые три секунды для их последующего анализа. Также существует более длительный процесс выборки признаков, который должен каждые 24 часа обнаруживать медленно происходящие и длительные по времени аномалии.

Модуль классификации соотносит новые правила ассоциации к нормальным или аномальным событиям. Некоторые из аномальных событий могут впоследствии быть классифицированы как атаки. В работе используется функция плотности распределения Дирихле. Она позволяет оценить значения для таблиц контингентности с большим количеством нулей.

Преимуществами системы является работа в режиме реального времени и обнаружение аномалий (а не злоупотреблений).

Метод на основе MAP-сплайнов позволяет построить более точную аппроксимацию поведения обычного пользователя или злоумышленника по указанным параметрам. С данной целью выбирается набор базисных функций, и находятся коэффициенты в линейном разложении по заданному базису и обучающим векторам. MAP-сплайны и метод опорных векторов показывают большую эффективность в распознавании 4 классов соединений по сравнению с нейронными сетями.

Методы вычислительного интеллекта. Под искусственной нейронной сетью понимается набор обрабатывающих элементов – нейронов, которые связаны между собой синапсами и преобразующими на выбор входных значений в совокупность желаемых выходных значений. Нейронные сети чаще всего применяются в таких технологиях, как распознавание образов, криптографии, теории управления и сжатие

данных. Они обладают способностью обучить по образу и обобщению из зашумленных и неполных данных.

В данной статье познакомимся с моделями нейронных сетей:

- Многослойные сети прямого распространения;
- Радиально-базисные сети;
- Рекуррентные сети;
- Самоорганизующиеся карты.

Для обучения нейронных сетей существует несколько методов. В статье «Системы обнаружения вторжений с использование адаптивных регрессионных сплайнов» предоставлено 12 алгоритмов их обучения. Наиболее популярным методом при обучении многослойным нейронным сетям прямого распространения является метод обратного распространения ошибки. Данный метод представляет собой градиентный спуск с минимизацией среднеквадратичной шибки на каждой итерации своего выполнения.

В других статьях для обнаружения атак используется многослойная нейронная сеть с двумя скрытыми слоями и выходным слоем, который состоит из трех нейронов. В качестве обучающего множества была выбрана база данных DARPA. Также в этой базе данных была показана многоуровневая нейронная сеть, в которой каждый из трех уровней представляет собой отдельный многослойный перцептрон, у которого распределительный слой состоит из 30 нейронов.

Дж. Кеннеди применял трехслойную нейронную сеть как бинарный классификатор соединений. Обучающим множеством являлся сетевой трафик, который был получен с помощью сетевого сканера. Оно насчитывало около 10 000 образцов соединений, 3 000 из которых являлись смоделированными вторжениями.

Радиально-базисные нейронные сети – класс нейронных сетей, базирующиеся на вычислениях расстояний от входного вектора до центров нейронов скрытого слоя. Из-за того, что радиально-базисные сети обладают простой структурой, они требуют меньше всего вычислительных ресурсов и времени на обучение. Данные сети подходят для решения задач с большим объемом выборки.

Рекуррентные нейронные сети позволили включить элемент память в модель нейронных сетей. Авторы статьи «Система обнаружения вторжений в реальном времени на основе поведения обучающей программы» применяли данную модель для предсказания следующей последовательности системных вызовов.

Самоорганизующиеся карты, или карты Кохонена, являются однослойными сетями прямого распространения, выходной слой которых

представляет собой n-мерную решетку (как правило, i=2 или i=3). После обучения такие сети группируют входные векторы со схожими признаками в отдельные кластеры. В некоторых статьях предлагают использовать данного рода сети для обнаружения аномалий. Для этой цели производился сбор данных, который описывает легитимное поведение пользователей и включает характеристики системных вызовов внутри одного и того же UNIX процесса.

Также для классификации записей из набора данных DARPA используется радиально-базисная нейронная сеть, первые два слоя которой представляют собой самоорганизующиеся карты. Результаты экспериментов показали, что данная модель имеет заметно лучшие показатели классификации по сравнению с радиально-базисными нейронными сетями на наборе данных DARPA.

Гибридные методы. Суть данных подходов заключается в реализации разных схем объединения базовых классификаторов, позволяющий нивелировать недостатки их функционирования по отдельности. Промежуточные результаты выходных значений являются вспомогательными при формировании решающего правила верхнеуровневыми классификаторами.

Существуют три классификатора:

- Дерево решений;
- SVM;
- Комбинация дерева решений и SVM (Гибрид).

Работа гибридного классификатора состояла из двух фаз. Для начала тестовые данные подавались на вход решающих деревьев, которые генерировали узловую информацию. Затем тестовые данные вместе с узловой информацией обрабатывались SVM, который выдавал результат классификации. Сутью данного подхода является исследование того, насколько узловая информация от дерева решений улучшит эффективность SVM. В случае расхождения результатов классификации, полученных с помощью этих трех методов, окончательный ответ выдавался на основе взвешенного голосования.

Также используются искусственные иммунные детекторы и самоорганизующиеся карты Кохонена. Во время выполнения система отслеживает сетевые соединения и для каждого из них формирует вектор признаков. Первый классификатор обучен по алгоритму отрицательного отбора. Поэтому любой вектор, отличный от своих клеток, считается аномальным и подается на вход самоорганизующихся карт Кохонена. Второй классификатор отображает этот вектор на нейрон внутри кластера множества атак, имеющих общие свойства. Тем самым атаки

обнаруживаются детекторами аномалий еще до проецирования на самоорганизующуюся карту.

Другим гибридным решением к задаче обнаружения вторжений является комбинирование нескольких нейронных сетей в единый классификатор. Итоговый классификатор представляется как композиция последовательно построенных на разных выборках классификаторов и процедуры простого голосования. Как результат уровень классификации удалось повысить примерно на 1,6% по сравнению с классификаторами, взятыми по отдельности.

В статье [83] описывается двухуровневая схема обнаружения и классификации атак. Несколько адаптивных нейро-нечетких модулей объединены вместе. Каждый из них предназначен для обнаружения только одного класса соединений и обрабатывает параметры записей KDD Cup 99. Итоговая классификация выполняется нечетким модулем принятия решений, который реализует систему нечеткого вывода Мамдани с двумя функциями принадлежности. Задачей этого модуля является определение того, насколько аномальной является обрабатываемая запись. Ее класс соответствует классу нечеткого модуля первого уровня с наибольшим выходным значением.

Предложения по использованию методов интеллектуального анализа данных (ИАД) в задачах обнаружения сетевых аномалий. На данный момент методы интеллектуального анализа данных применяются во многих сферах: идентификации биометрических показателей, оптическом распознавании символов, построении рекомендательных сервисов, обнаружении спама. Однако, в некоторых случаях применение данных методов вызывает ряд трудностей с выявлением аномалий. Обнаружение аномалий представляет собой детектирование ранее не встречавшихся атак, в то время как методы ИАД направлены на поиск взаимосвязей и закономерностей в сетевом трафике, выявлении активности, которая похожа на ранее появляющуюся при обучающей выборке. Применение инструментов ИАД в готовом виде «из коробки» к задаче обнаружения аномалий приводит к большому числу ложных срабатываний и пропусков атак. В первую очередь это обусловлено тем, что сетевой трафик постоянно меняется изо дня в день. Также сложно отследить цикличность или сезонность такого изменчивого поведения. Поэтому одним из подходов к решению этой проблемы с использованием методов ИАД является динамическая подстройка интеллектуальных детекторов к изменяющимся условиям.

Также проблемой в области обнаружения аномалий является задача определения того, что же все-таки является нормальным трафиком, а что

нет. Ведь если надо обнаруживать аномалии, то необходимо определить фильтр нормальности, чтобы максимально полно описать нормальную деятельность, откидывать все ненормальные действия и обучать модели только на нормальных данных.

Самый важный вопрос в данной области – как выбирать признаки, которые характеризуют нормальный трафик и аномалии, пригодные для обучения ИАД. Нужно опытным путем сначала попробовать строить временные последовательности с наиболее полным набором признаков, характеризующих наблюдаемые явления в сети, и далее на основе экспериментов отсекать все инвариантные свойства, которые сохраняются при смене типа трафика, как заведомо неинформативные. После этого обучение будет проводиться на наборе оставшихся атрибутов.

Таким образом, методы ИАД применять для задания пороговых значений, преобразования (предобработки) входных параметров, к примеру, при помощи следующих методов ИАД: метода главных компонент (PCA, principal component analysis), сингулярного разложения (SVD, singular value decomposition), внешне не связанных уравнений (SUR, seemingly unrelated regressions). А также можно использовать их совместно с сигнатурными методами на основе правил.

В данной статье был проведен сравнительный анализ методов обнаружения сетевых атак. Эти подходы часто используются учеными при разработке различных систем обнаружения атак. Предложена классификация данных методов по группам в зависимости от подхода к решению вопроса выявления аномалий.

Более перспективными направлениями при разработке систем обнаружения аномалий в сети является создание гибридов из различных подходов, позволяющая совмещать в себе преимущества сигнатурных методов и применение технологий больших данных. Самым главным требованием, которое предъявляется к решениям, является обеспечение адаптивной и масштабируемой аналитической обработки событий, которые в последующем обеспечат полную безопасность данных в реальном или близком к реальному масштабе времени.

Использованные источники

1. Информационная технология. Методы и средства обеспечения безопасности [Текст]: ГОСТ Р ИСО/МЭК 15408 – 1 - 2008. Введ. 2009-10-01. – М.: Стандартинформ, 2009.

2. Лукацкий А.В. Обнаружение атак [Текст]: СПб.: БХВ-Петербург. 2003. 608 с.

3. Kumar S., Spafford E.H. A Pattern Matching Model for Misuse Intrusion Detection [Текст]: Proceedings of the 17th National Computer Security Conference, 1994. pp. 11–21.

4. Ghorbani A.A., Lu W., Tavallaee M. Network Intrusion Detection and Prevention: Concepts and Techniques [Текст]: Springer Science & Business Media. 2009. 212 p.

5. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей [Текст]: М.: ИД «ФОРУМ»: ИНФРА-М. 2008. 416 с.

6. Wespi A. Towards a taxonomy of intrusion-detection systems // Computer Networks. 1999. vol. 31. Issue 8. pp. 805–822.

7. Mukkamala S., Sung A.H., Abraham A., Ramos V. Intrusion Detection Systems Using Adaptive Regression Splines [Текст]: Sixth International Conference on Enterprise Information Systems. 2006. pp. 211–218.

8. Котенко И.В., Нестерук Ф.Г., Чечулин А.А. Комбинирование механизмов обнаружения сканирования в компьютерных сетях [Текст]: Вопросы защиты информации. 2011. № 3. С. 30–34.