УДК 004.056

А.А. Браницкий, И.В. Котенко

АНАЛИЗ И КЛАССИФИКАЦИЯ МЕТОДОВ ОБНАРУЖЕНИЯ СЕТЕВЫХ АТАК

Браницкий А.А., Котенко И.В. **Анализ и классификация методов обнаружения сетевых атак.**

Аннотация. В работе рассматриваются различные методы обнаружения сетевых атак. Основное внимание уделяется построению обобщенной классификационной схемы методов обнаружения сетевых атак, представлению сущности каждого из рассмотренных методов и их сравнительному анализу в рамках предложенной классификационной схемы.

Ключевые слова: сетевые атаки, обнаружение злоупотреблений, обнаружение аномалий, сетевой трафик.

Branitskiy A.A., Kotenko I.V. **Analysis and Classification of Methods for Network Attack Detection.**

Abstract. Different methods of detection of network attacks are considered in the paper. The paper focuses on the construction of the generalized classification scheme of methods of network attack detection, description of each of the above methods and their comparative analysis within the proposed classification scheme.

Keywords: network attacks, misuse detection, anomaly detection, network traffic.

1. Введение. Стремительное развитие компьютерных сетей и информационных технологий вызывает ряд проблем, связанных с безопасностью сетевых ресурсов, которые требуют новых подходов. В настоящее время вопросы построения систем обнаружения атак представляют собой актуальное направление в области информационных технологий. Существует множество работ, посвященных тематике обнаружения и классификации атак с применением разнообразных методов, которые включают традиционные подходы на основе соответствия сигнатурным образцам и адаптивные модели с применением методов интеллектуального анализа данных (ИАД). Большинство этих работ были сделаны достаточно давно, и некоторые из них имеют ограниченный аспект в форме охвата только конкретной предметной области, а именно, обнаружения злоупотреблений или аномалий.

Настоящая работа нацелена на анализ известных методов для обнаружения и классификации сетевых атак и построение обобщенной схемы классификации этих методов. Статья имеет следующую структуру. В разделе 2 представлена схема классификации методов. В разделе 3 рассмотрены поведенческие методы. Раздел 4 посвящен описанию методов на основе знаний. Раздел 5 содержит методы машинного обучения. Методы вычислительного интеллекта представлены в разделе 6. Гибридные методы рассмотрены в разделе 7. В разделе 8 предложены

рекомендации по применению методов ИАД в задачах обнаружения сетевых аномалий.

2. Схема классификации методов обнаружения атак. Общепринятая классификация систем обнаружения атак по способам выявления атак включает системы обнаружения аномалий и системы обнаружения злоупотреблений [1]. Одной из классических работ в области обнаружения злоупотреблений является работа [2]. На рисунке 1 представлена схема обнаружения сетевых аномалий [3] на основе показателей сетевого трафика.

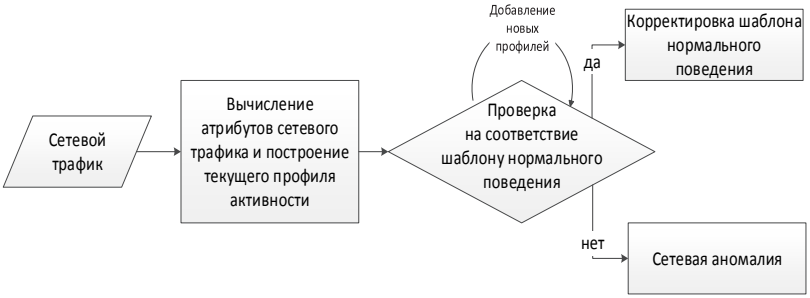

Рис. 1. Схема обнаружения сетевых аномалий

Общий алгоритм выявления сетевых аномалий может быть описан следующим образом. Данными для анализа является сетевой трафик, представленный как набор сетевых пакетов, в общем случае фрагментированных на уровне IP. Собранные сырые данные в дальнейшем послужат источником при формировании необходимой информации для последующего анализа. Так, полученные данные могут быть агрегированы за определенный временной интервал и нормализованы с целью задания признаковых атрибутов общего вида, которые потребуются при построении текущего профиля активности. Созданный набор признаков сравнивается с набором характеристик нормальной деятельности объекта (пользователя или системы) — шаблоном нормального поведения. Если наблюдается существенное расхождение сравниваемых параметров, то фиксируется сетевая аномалия. В противном случае происходит уточнение шаблона нормального поведения посредством изменения параметров его настройки с учетом текущего наблюдаемого профиля сетевой активности.

Описанный выше алгоритм может включать несколько вариантов исполнения для реализации подсистемы проверки на соответствие шаблону нормального поведения. Простейшим из них является процедура сравнения с пороговой величиной, когда накопленные результа-

ты, описывающие текущую сетевую активность, сравниваются с экспертно заданной числовой планкой. В этом подходе случай превышения значений рассматриваемых параметров указанной границы является признаком сетевой аномалии. Остальные подходы, включая этот, рассмотрены в разделе 3.

Стоит отметить, что построение шаблона нормального поведения является трудоемкой задачей и зачастую не всегда выполнимой. Так, на практике оказывается, что не каждое аномальное поведение является атакой [4]. К примеру, администратор сети может применять отладочные утилиты, такие как ping, traceroute, mtr, для диагностики сетевого окружения. Действия подобного рода не преследуют каких-либо нелегальных умыслов, однако системы обнаружения аномалий распознают эту деятельность как аномальную сетевую активность.

На рисунке 2 показана схема обнаружения злоупотреблений [3] в сетевом трафике.

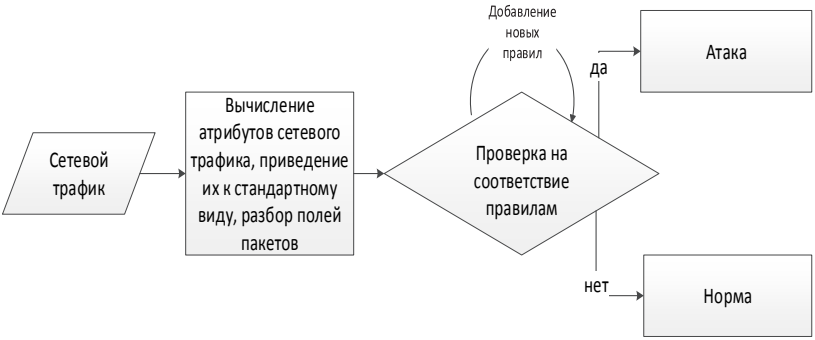

Рис. 2. Схема обнаружения злоупотреблений в сети

Обнаружение злоупотреблений позволяет идентифицировать несанкционированные действия, если имеется их точное представление в виде шаблонов атак. Здесь под шаблоном атаки понимается некоторая совокупность явно описывающих конкретную атаку действий (правил сопоставления, вывода), применяя которые к признакам и полям идентифицируемого объекта можно получить однозначный ответ о его принадлежности к этой атаке. Как и в схеме обнаружения сетевых аномалий, при обнаружении злоупотреблений первичными данными для анализа является сетевой трафик. Выделенные атрибуты и поля сетевых пакетов передаются в модуль, который выполняет поиск и проверку на соответствие входных данных правилам и оповещает о наличии угрозы в случае положительного срабатывания одного из правил.

Ключевой проблемой при создании любой системы обнаружения злоупотреблений является вопрос об эффективном проектировании механизма задания правил. Понятно, что создание исчерпывающей базы правил для выявления всевозможных атак является невозможным в силу нескольких факторов. Один из этих факторов заключается в том, что описание различных вариаций атакующих действий негативно сказывается на производительности системы. А поскольку даже несущественные изменения в атаке приводят к невозможности ее обнаружения методами на основе злоупотреблений, то задаваемые правила должны быть универсальными и покрывать как можно большее число известных модификаций сетевых атак.

Подытоживая сказанное, отметим, что методы обнаружения злоупотреблений являются эффективным инструментом для выявления известных типов атак, но их применимость по отношению к новым атакам, а также к модификациям известных атак является безрезультативной.

Классическими работами в области обнаружения аномалий являются работы [5, 6].

Классификация методов обнаружения атак, предлагаемая в настоящей работе, схематически показана на рисунке 3. Для ее построения был проведен анализ большого перечня работ, в том числе [7-12], который позволил уточнить предложенные в них таксономии и схемы известных методов обнаружения сетевых атак.

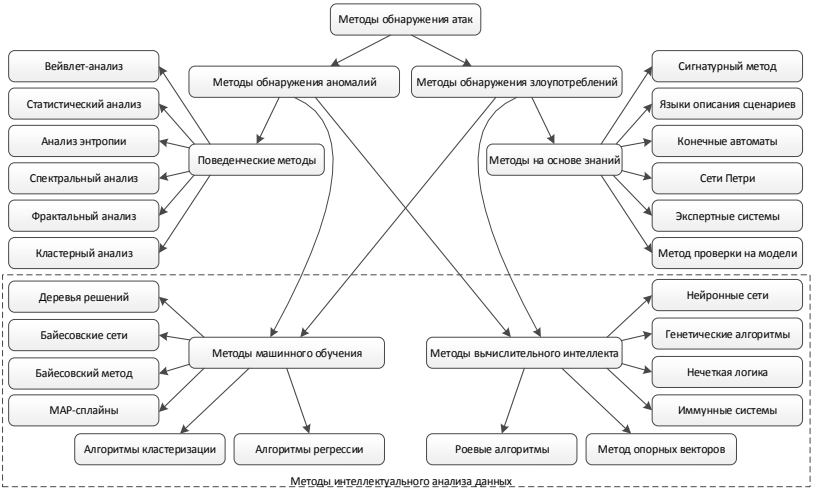

Рис. 3. Классификация методов обнаружения атак

Данная схема разбиения является условной и не претендует на полноту: некоторые из подходов могут относиться к нескольким группам. В частности, экспертные системы и конечные автоматы могут использоваться для обнаружения аномалий, но в большинстве случаев они применяются именно для обнаружения злоупотреблений. Также такие методы вычислительного интеллекта, как нейронные сети и метод опорных векторов, зачастую причисляют к методам машинного обучения. В схеме, соответствующей рисунку 3, выбрано такое разбиение, при котором методы ИАД классифицируются по критерию их принадлежности к биоподобным алгоритмам и поэтому содержат в себе два класса: методы вычислительного интеллекта и методы машинного обучения. Ниже в соответствующих разделах рассмотрена каждая группа представленных методов.

3. Поведенческие методы. Поведенческими методами [13] называются методы, которые основаны на использовании информации о нормальном поведении системы и ее сравнении с параметрами наблюдаемого поведения. Представленная группа методов ориентирована на построение модели штатного, или нормального, функционирования системы или пользователя. В процессе своей работы системы, использующие данный подход, сравнивают текущие показатели активности с профилем нормальной деятельности, и случай значительных отклонений может рассматриваться как свидетельство наличия атаки.

Данные методы характеризуются наличием ложноположительных срабатываний, которые объясняются в первую очередь сложностью точного и полного описания множества легитимных действий пользователей. Кроме того, для большинства подобных систем характерно и необходимо проведение этапа предварительной настройки, во время которого система «набирается опыта» для создания модели нормального поведения. Продолжительность такого интервала для сбора данных может занимать несколько недель, а иногда и несколько месяцев. Указанные недостатки зачастую являются основными причинами отказа от применения систем, построенных на основе поведенческих методов, в пользу тех систем, которые используют точное представление нарушений безопасности в сети.

В данной работе к поведенческим методам отнесены следующие методы обнаружения атак:

– вейвлет-анализ;
– статистический анализ;
– анализ энтропии;
– спектральный анализ;
– фрактальный анализ;

– кластерный анализ.

Вейвлет-анализ заключается в построении коэффициентов, используемых в разложении исходного сигнала по базисным функциям. В качестве сигнала может рассматриваться интенсивность сетевого трафика [14] или данные о корреляции IP-адресов назначения [15]. Выполнение вейвлет-преобразования позволяет выделить наиболее весомую информацию как сигнал, соответствующий колебаниям с высокой амплитудой, и игнорировать менее полезную информацию в колебаниях с низкой амплитудой как шумовую составляющую.

В [16] авторы в качестве исходных данных использовали агрегированные за пятиминутные интервалы средние значения следующих величин: количество байт в секунду, количество пакетов в секунду, количество потоков в секунду, величина среднего размера TCP-пакета. В каждом случае собранные данные представляли собой дискретную последовательность частотно-временного сигнала, который согласно предложенному алгоритму вейвлет-анализа был декомпозирован в виде иерархии нескольких слоев (strata). Для каждого из извлеченных сигналов переменная времени являлась независимой. Наличие резких амплитуд в каждом из представленных сигналов соответствовало определенным группам аномалий. Так, были выделены следующие группы сетевых аномальных событий:

– аномалии, вызванные ошибками в настройках сетевого оборудования, а также сбоем в работе оборудования (G_1);

– сетевые атаки, представленные классом «отказ в обслуживании» (G_2);

– перегрузки в сети (flash crowd), которые возникают вследствие резких всплесков, например, в моменты увеличения легитимных запросов на скачивание новых релизов программного обеспечения (G_3);

– прочие аномалии, к числу которых относятся обмен большим количеством данных, ошибки во время записи трафика на сенсоре или отправки данных коллектору NetFlow, дающего возможность анализа сетевого трафика на уровне сеансов (G_4);

Были выделены три составляющих компонента первичного сигнала [16]. Низкочастотный компонент сигнала захватывал продолжительные по времени сетевые аномалии, которые могут длиться от нескольких дней. Среднечастотная часть имела нулевое математическое ожидание и была предназначена для анализа колебаний в пределах одного дня. Высокочастотная часть соответствовала небольшим кратковременным изменениям, которые могут рассматриваться как шум.

После разбиения исходного сигнала авторы [16] применяют к первым двум его компонентам процедуру вычисления локальной дис-

персии в рамках скользящего окна размером 3 часа. Далее применяется метод порогового анализа к взвешенной сумме этих компонентов. Аномалия идентифицируется в случае, если пиковая точка последнего сигнала превысила заданный порог.

В результате исследования был сделан вывод о том, что представленные типы аномальных событий могут быть идентифицированы на конкретных, присущих им частотах. Так, крупнозернистые аномалии классов G_1, G_2 и G_4 распознаются на высоких и средних частотах, в то время как аномалиям класса G_3 соответствуют низкочастотные и среднечастотные сигналы.

Недостатками вейвлет-анализа являются неоднозначность выбора базисных функций, большая вычислительная сложность при расчете коэффициентов разложения сигнала. Кроме того, нетривиальной является задача правильного задания размера окна. Как было отмечено в [16], если размер скользящего окна намного превышает продолжительность аномалии, то соответствующий ей частотный всплеск может быть сглажен, и тем самым атака будет пропущена. В противном случае, если величина окна слишком малая, то неизбежен поток бессмысленных аномалий.

Статистический анализ [6] является ядром методов обнаружения аномалий в сети. К этой группе относят следующие методы:

– цепи Маркова;
– метод хи-квадрат (χ^2);
– метод среднеквадратических отклонений;
– анализ распределений интенсивности передачи/приема пакетов;
– анализ временных рядов;
– пороговый анализ.

В таблице 1 приведено описание этих подходов.

Отметим, что в статистических системах важную роль играет правильный выбор контролируемых параметров, характеризующих отличия в нормальном и аномальном трафиках. Может получиться так, что из-за неправильного выбора количества наблюдаемых параметров модель описания поведения субъектов в системе окажется неполной или избыточной. Это приводит к пропуску атак или ложным срабатываниям в системе.

Преимуществами статистических систем является их адаптация к изменению поведения пользователя, а также способность к обнаружению модификаций атаки. Среди недостатков можно отметить высокую вероятность возникновения ложных сообщений об атаках и зависимость от порядка следования событий.

Таблица 1. Статистические методы обнаружения сетевых атак

Метод	Краткое описание метода	Преимущества метода	Недостатки метода	Пример применения
Цепи Маркова	Используется матрица перехода состояний для задания возможных связок между допустимыми действиями легитимного пользователя. Элементы матрицы — вероятности смены состояний. Событие является аномальным, если вероятность его наступления слишком мала. Вероятность наступления события сводится к вычислению произведения вероятностей отдельных составляющих этого события [17].	Возможность получения вероятности атаки. Сохранение промежуточных состояний для дальнейшего анализа вредоносных действий. Возможность применения упреждающих действий по ликвидации следующих шагов развития атаки.	Экспоненциальное увеличение числа состояний моделируемой цепи с ростом ее порядка. Необходимость в периодическом изменении параметров модели с целью ее адаптации к изменяющемуся поведению легитимного пользователя.	Обнаружение многошаговых атак. Обнаружение аномалий, которые не соответствуют заданным в цепочке правил спецификациям. Обнаружение медленных, распределенных во времени атак.
Метод χ^2	Тест по критерию χ^2 применяется для проверки того, что некоторая выборка удовлетворяет определенному закону распределения. По правилу трех сигм для нормально распределенной случайной величины, соответствующей измерениям трафика без аномалий, вычисляется верхняя граница изменения ее значения χ^2. Аномалия фиксируется в случае превышения этой границы значением χ^2 наблюдаемой величины [18].	Высокая теоретическая точность обнаружения в случае нормально распределенных случайных величин (99.7% для 95%-го доверительного интервала).	Предположение о нормальном распределении векторов наблюдаемых измерений, соответствующих трафику без аномалий. Необходимость задания наиболее полной выборки измерений нормального трафика.	Обнаружение сетевых аномалий, характеризующихся увеличением значений наблюдаемых параметров.
Метод среднеквадратических отклонений	На основе n предыдущих значений наблюдаемых параметров строится доверительный интервал [m-k·s, m+k·s] для каждой из наблюдаемых величин (m – математическое ожидание, s – среднеквадратическое отклонение, k – регулируемый коэффициент, представленный как отношение z-значения к квадратному корню из объема выборки n). Событие считается аномальным, если значения его параметров не принадлежат этому интервалу.	Наличие адаптивной способности, позволяющей подстраиваться под изменения сетевого окружения.	Возможность постепенного переобучения системы со стороны злоумышленника с целью ее введения в заблуждение о нормальном поведении пользователя. Необходимость создания репрезентативной выборки нужного размера, представленной исключительно легитимным трафиком.	Обнаружение широкого класса атак, характеризующихся резкими амплитудными всплесками относительно стационарного положения.

Анализ распределений интенсивности передачи/приема пакетов	Для данной сети строится модель, описывающая распределение интенсивности передачи пакетов (логнормальное, гамма, пр.). Для трафика без аномалий находятся параметры этого распределения. В тестовом режиме параметры новой построенной модели сравниваются с параметрами эталонной модели. Сетевая аномалия регистрируется в случае значительных расхождений вычисленных параметров.	Возможность наглядного визуального представления аномалии в сети с помощью графиков и гистограмм.	Зависимость качества обнаружения от выбора величины допустимого изменения параметров.	Обнаружение аномальных выбросов сетевого трафика. Обнаружение атак «отказ в обслуживании» типа flooding. Выявление атак, вызывающих перегрузки сетевого оборудования.
Анализ временных рядов	Временной ряд представляет собой последовательность наблюдений, записанных в определенный момент времени [19]. Вычисленные показатели трафика соответствуют элементам дискретного ряда. Для набора этих измерений строится прогноз с использованием алгоритмов экспоненциального сглаживания, скользящего среднего или авторегрессии, позволяющих выявлять закономерности изменения трафика.	Возможность динамического и долгосрочного прогнозирования трендов, задающих изменения нормального функционирования системы. Возможность обнаружения постепенных, но значительных отклонений от нормального поведения.	Сложность выбора прогнозирующей функции. Усложнение описательной модели для учета сезонности наблюдаемого временного ряда. Низкая эффективность обнаружения атак для случая рядов, не обладающих свойством стационарности.	Обнаружение кратковременных фоновых атак «отказ в обслуживании», приводящих к аномальным всплескам сетевой активности.
Пороговый анализ	Для наблюдаемых параметров задается допустимый диапазон изменения его значений. Нахождение вне рамок этого диапазона соответствует аномальному поведению. Простейшей модификацией, позволяющей снизить количество ложных срабатываний, является добавление счетчика, который накапливает события «выпадания» наблюдаемых параметров из диапазона. При превышении счетчиком определенного значения фиксируется факт наличия аномалии.	Простота реализации и настройки. Отсутствие этапа предварительного обучения. Простота интерпретации полученных результатов, свидетельствующих о нормальности/аномальности событий в сети.	Необходимость тонкого задания числового порога, требующего знаний эксперта и напрямую влияющего на качество обнаружения. Отсутствие адаптивных механизмов для автоматического выбора порога. Необходимость тщательного анализа полученных результатов вследствие возможных пропусков атак и ложных срабатываний.	Обнаружение простых видов атак «подбор пароля». Обнаружение атак «отказ в обслуживании» на основе сравнения интегральных характеристик трафика. Обнаружение аномалий, характеризующихся необычным временем суток для активности в сети.

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

Энтропия множества X определяется следующим образом [20]:

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

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

Суть метода заключается в построении модели, которая максимизировала бы значение энтропии. Это соответствует тому предположению, что с увеличением числа уникальных записей происходит их равномерное распределение относительно выбранных классов множества X, что приводит к увеличению энтропии.

Для обнаружения аномалий в [21] сперва применяется метод максимума энтропии для создания нормальной модели, в которой выделенные классы сетевых пакетов обладают наилучшим равномерным распределением. Далее применяется условная энтропия для выявления отличий между распределением классов пакетов в текущем трафике по сравнению с распределением, найденным в результате метода максимума энтропии.

Спектральный анализ является частным случаем вейвлет-преобразования и позволяет выделять наиболее информативные составляющие исследуемого процесса посредством изменения размерности исходного пространства признаков. Для этих целей анализируется ковариационная матрица элементов исследуемого процесса при помощи метода главных компонент, гусеницы или сингулярного спектрального анализа [22].

Данный подход основан на том предположении, что полученные компоненты аномального трафика отличаются от компонент обычного трафика. Главные компоненты выбираются таким образом, чтобы они соответствовали наибольшей изменчивости исходного процесса. Остальные компоненты могут быть рассмотрены как составляющие шума.

Фрактальный анализ основан на предположении, что сетевой трафик удовлетворяет свойству самоподобия [23], ключевыми 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 $X = \{x_1, \dots, x_N\}$ со средним значением $\bar{x} = \frac{1}{N} \cdot \sum_{i=1}^{N} x_i$, $R = \max_{1 \le i \le N} x_i - \min_{1 \le j \le N} x_j$ — размах отклонения (изменчивость) ряда, $S = \sqrt{\frac{1}{N-1} \cdot \sum_{i=1}^{N} (x_i - \bar{x})^2}$ — 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 [24].

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 [25].

4. Методы на основе знаний. К методам на основе знаний относят такие методы, которые в контексте заданных фактов, правил вывода и сопоставления, отражающих признаки заданных атак, производят действия по обнаружению атак на основе заложенного механизма поиска [13]. В качестве процедуры поиска могут применяться сопоставление по образцу, аппарат регулярных выражений, логический секвенциальный вывод, анализ перехода состояний и т.д. Своим названием эти методы обязаны тем, что системы, основанные на их применении, работают с базой знаний, в которой включены описания уже известных атак. Здесь база знаний представлена хранилищем, содержащим записи экспертов с поддержкой логики их обработки и интерпретации (т.е. характеризуется наличием подсистемы логического вывода).

Как уже отмечалось в разделе 2, если отсутствуют точные знания о модификациях вредоносной активности, то данные методы не справляются с обнаружением различных вариаций этой вредоносной деятельности.

В *сигнатурных методах* системные события представляются в виде цепочек символов из некоторого алфавита. Суть этих методов заключается в задании множества сигнатур атак в виде регулярных выражений (regular expressions) или правил на основе сопоставления с образцом (pattern matching) и проверке соответствия наблюдаемых событий этим выражениям. Типичными представителями систем, в которых реализован такой метод, являются Snort [26] и Suricata [27].

Основное преимущество сигнатурного метода заключается в том, что обнаружение известных образцов аномальных событий осуществляется максимально эффективно. Но в то же время использование базы сигнатур большого объема отрицательно влияет на производительность системы обнаружения [1].

Языки описания сценариев предоставляют гибкий механизм обработки контролируемых данных, который заключается в возможности написания собственных скриптов. Такой подход позволяет выявлять такие события, которые трудны для описания при помощи обычных сигнатурных инструментов анализа [7].

Метод на основе *конечных автоматов* (КА) дает возможность моделировать атаки в виде взаимосвязанной сети из состояний и переходов. Вторжение считается успешно реализованным, если последовательность действий атакующего приводит систему из некоторого устойчивого состояния в скомпрометированное. Каждое состояние можно рассматривать как слепок параметров безопасности, а переходы между ними соответствуют успешному срабатыванию события, которое приводит систему в новое состояние. Фактически каждое наблюдаемое событие применяется к нескольким экземплярам КА, каждый из которых представляет собой определенный сценарий атаки.

Одной из первых попыток в реализации этого подхода считается работа [28]. Разработанная авторами [28] программная система USTAT предназначалась для обнаружения атак на UNIX-хосты и включала несколько компонентов. На первом уровне осуществлялся сбор данных из журнала регистрации событий. Полученные данные помещались в постоянное хранилище и подавались на вход препроцессору. Последний представляет собой два отдельных компонента: детектор аномалий на основе профиля пользователя или системы и так называемый STAT-компонент. Каждый модуль препроцессора независимо анализирует события безопасности на наличие скомпрометированного содержимого. В случае выявления угроз оба модуля предоставляют необходимую информацию администратору. Кроме того, администратор имеет непосредственный доступ к сырым данным из журнала аудита.

Сам STAT-компонент включает в себя три модуля: базу знаний, подсистему логического вывода и подсистему принятия решений. Сперва препроцессор обрабатывает сырые данные из журнала регистрации событий и подает их на вход подсистеме вывода, которая отслеживает переходы и сравнивает их со сценариями из базы знаний. Затем подсистема принятия решений определяет действия, которые должны быть выполнены при смене состояния.

Другим примером системы обнаружения злоупотреблений на основе анализа переходов состояний является IDIOT (Intrusion Detection In Our Time), в которой применяется метод раскрашенных *сетей Петри*. Сценарии вторжений кодируются в шаблоны IDIOT, и события безопасности проверяются путем их сопоставления с этими шаблонами [29].

Преимущество данного метода заключается в возможности визуального представления атаки в виде диаграмм перехода состояний, а также в способности системы обнаруживать атаку до ее фактического совершения. Из недостатков можно отметить сложность реализации.

Функционирование *экспертных систем* основано на применении правил вывода к данным о входных событиях. Они представляют собой системы, принимающие решение о принадлежности события к определенному классу атак на основании заданных продукционных правил.

Общий вид продукционного правила следующий [2]: $IF\ condition\ THEN\ action$. В посылке данного правила содержится логическое условие, необходимое для совершения атаки. Когда все условия в левой части правила удовлетворены, выполняются действия, указанные в сукцеденте.

Предполагается, что перед использованием таких систем администратор должным образом их настраивает, задавая необходимые правила. Подобные системы дают возможность использовать человеческий опыт в компьютерных приложениях, которые затем будут применять эти знания для распознавания активностей, соответствующих определенным характеристикам атак.

Достоинства данного метода — возможность отделения управляющей части правила от части, задающей решение, высокая скорость работы и возможность обеспечения отсутствия ложных тревог [2]. Недостатки — неспособность к обнаружению неизвестных атак, зависимость системы от полноты, корректности и актуальности правил, заложенных в базу знаний, снижение эффективности работы с увеличением объема данных.

Также *метод проверки на модели* может быть использован для обнаружения сетевых злоупотреблений [30].

5. Методы машинного обучения. Методы машинного обучения, как и методы вычислительного интеллекта, применяются как при обнаружении аномалий, так и при обнаружении злоупотреблений. Это объясняется тем, что указанные подходы в качестве исходных данных для обучения зачастую используют шаблоны как нормального, так и аномального поведения в сети.

В [31] авторы предложили замену стандартному модулю обнаружения в системе Snort *деревьями решений*. Эксперименты были проведены на наборе данных DARPA [32] и показали увеличение скорости обработки pcap-файлов, используемых для анализа сетевых пакетов, в среднем на 40,3% по сравнению со стандартным модулем.

Одним из наиболее часто используемых подходов для обнаружения вторжений являются байесовские сети. *Байесовская сеть* — это

модель, которая кодирует вероятностные отношения между рассматриваемыми событиями (переменными) и предоставляет некоторый механизм для вычисления условных вероятностей их наступления [33]. Частный случай этой модели — *наивный байесовский классификатор* (*байесовский метод*) со строгими предположениями о независимости входных переменных. Классификатор позволяет оценить апостериорную вероятность принадлежности экземпляра заданному классу на основе безусловной теоремы Байеса.

В [34] применяются псевдобайесовские оценочные функции для определения априорных и апостериорных вероятностей новых атак. Наивный байесовский классификатор используется для классификации сетевых образцов. В [34] утверждается, что вследствие свойств предложенного метода системе не нужны предварительные знания о шаблонах новых атак.

Предложенная в [34] система ADAM состоит из трех частей: модуля предобработки, интеллектуального модуля и модуля классификации.

Первый модуль собирает данные из TCP/IP трафика и извлекает информацию из каждого соединения в соответствии со следующей схемой $\langle time\_stamp, src\_ip, src\_port, dst\_ip, dst\_port, conn\_status \rangle$, где $time\_stamp$ — временная метка, src_ip — IP-адрес источника, src_port — порт источника, dst_ip — IP-адрес назначения, dst_port — порт назначения, $conn\_status$ — состояние соединения.

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: режиме обучения и режиме обнаружения. В первом режиме происходит построение профилей нормального поведения пользователей и системы, и генерируются правила ассоциации, которые будут использоваться для обучения модуля классификации. Во втором режиме интеллектуальный модуль получает ранее не встречавшиеся правила ассоциации, которые отличаются от профиля. Представлены три уровня работы интеллектуального модуля: обособленный уровень, уровень домена, а также уровень выборки признаков. Первый уровень имеет два режима: статический и динамический анализ. Первый режим используется во время нормальной работы системы, когда создается профиль для поведения системы. Второй режим использует метод скользящего окна для поэтапного анализа правил ассоциации. На уровне домена система отслеживает IP-адреса отправителя и получателя. Соединение считается подозрительным, если эти адреса принадлежат одной и той же подсети. На уровне признаков сис-

тема 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. В данных таблицах колонки соответствуют атрибутам образцов соединений, а строки указывают на класс обучающих данных, который является или нормальным соединением, или типом атаки. Таблица строится таким образом, что значение в ячейке на пересечении -ой строки и j-ой колонки указывает на количество образцов в обучающей выборке, для которых представлены i-ый класс соединения и j-ый атрибут. Кроме всех классов, представленных в обучающей выборке, добавляется строка в таблице сопряженности для обозначения дополнительного класса, представляющего новый тип атак. Значения в ячейках новой строки заполняются нулями. После чего применяются метод Дирихле, сглаживающий особенности в новой строке, и наивный байесовский классификатор.

Авторы отмечают два основных преимущества их системы — это работа в режиме реального времени и обнаружение аномалий (а не злоупотреблений).

Метод на основе *MAP-сплайнов* позволяет построить достаточно точную аппроксимацию поведения обычного пользователя или злоумышленника по заданным параметрам. С этой целью выбирается набор базисных функций, и находятся коэффициенты в линейном разложении по заданному базису и обучающим векторам. В [35] авторы предлагают строить классификаторы на основе MAP-сплайнов для распознавания 5 выбранных типов сетевых соединений, а также приводят показатели точности обнаружения на данных из набора DARPA 1998 для MAP-сплайнов, нейронных сетей и метода опорных векторов. Для тестирования использовалась выборка мощностью 6890 записей, для обучения применялось 5092 записи. Из приведенных результатов можно заключить, что MAP-сплайны и метод опорных векторов показывают большую эффективность в распознавании 4 классов соединений по сравнению с нейронными сетями.

Среди других подходов машинного обучения стоит отметить *алгоритмы кластеризации* [36, 37] *и регрессии* [38].

6. Методы вычислительного интеллекта. Искусственная *нейронная сеть* представляет собой набор обрабатывающих элементов — нейронов, связанных между собой синапсами и преобразующими набор входных значений в набор желаемых выходных значений. Нейронные сети применяются в широком спектре приложений: распознавании образов, теории управления, криптографии, сжатии данных. Нейронные сети обладают способностью обучения по образцу и обобщения из зашумленных и неполных данных. В процессе обучения происходит настройка коэффициентов, ассоциированных с синаптическими весами.

В данной работе представлен краткий обзор нескольких моделей нейронных сетей, а именно — многослойных сетей прямого распространения, радиально-базисных сетей, рекуррентных сетей и самоорганизующихся карт.

Для обучения нейронных сетей существует несколько методов. В [35] представлены 12 алгоритмов для их обучения. Одним из самых известных и наиболее используемых алгоритмов обучения многослойных нейронных сетей прямого распространения является метод обратного распространения ошибки. Этот алгоритм представляет собой градиентный спуск с минимизацией среднеквадратичной ошибки на каждой итерации своего выполнения.

В [39,40] для обнаружения вторжений используется многослойная нейронная сеть с двумя скрытыми слоями и выходным слоем, состоящим из трех нейронов. В качестве обучающего и тестового множества была выбрана база данных DARPA. Построенный на данной выборке классификатор был обучен распознавать два типа атак и нормальное соединение. В обеих работах для обучения нейросети используется алгоритм обратного распространения ошибки.

Другой работой, в которой используется эта же база данных, является [41]. В ней показана архитектура многоуровневой нейронной сети, в которой каждый из трех уровней представляет собой отдельный многослойный перцептрон, распределительный слой которого состоит из 30 нейронов. На каждом уровне осуществляется уточнение классификации соединения. Так, на первом уровне определяется, является ли данное соединение атакой или нормальным соединением. Второй и третий уровни отвечают за классификацию соответственно класса и подкласса атаки. Особенностью данного подхода является возможность получения необходимой степени детализации при классификации рассматриваемого соединения.

Дж. Кеннеди [42] использовал трехслойную нейронную сеть как бинарный классификатор сетевых соединений. Обучающее множество, представляющее собой сетевой трафик, полученный с помощью сете-

вого сканера, насчитывало около 10000 образцов соединений, среди которых 3000 записей являлись смоделированными атаками. Хотя этап обучения занимал 26.13 часа, результаты экспериментов показали высокую степень корректности распознавания.

Работы [43, 44] посвящены обнаружению аномалий с использованием нейронных сетей на основе данных, взятых из системного журнала аудита и лог-файлов отдельных приложений. В [43] для задания профиля каждого пользователя применялись наборы из наиболее распространенных команд и частота их использования, а в [44] также использовалась системная информация, в том числе объем системных ресурсов, время работы в системе и пр.

Радиально-базисные нейронные сети — класс нейронных сетей, который базируется на вычислении расстояния от входного вектора до центров нейронов скрытого слоя. Обладая более простой структурой по сравнению с многослойными нейронными сетями, радиально-базисные нейронные сети требуют меньше вычислительных ресурсов и времени для обучения, а значит, они идеально подходят для задач с большим объемом выборки. В [45] приводится обзор работ с применением радиально-базисных нейронных сетей к задачам обнаружения вторжений.

Изобретение рекуррентных нейронных сетей позволило включить элемент памяти в модель нейронных сетей. В [46] авторы использовали 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, $n = 2$ или $n = 3$). После обучения такие сети группируют входные векторы со схожими признаками в отдельные кластеры.

В [47, 48] предлагается использовать самоорганизующиеся карты для обнаружения аномалий. Для этих целей были собраны данные, описывающие легитимное поведение пользователей и включающие характеристики системных вызовов внутри одного и того же UNIX процесса. В [49-51] самоорганизующиеся карты используются для предобработки и кластеризации данных о сетевом трафике. Обработанные данные использовались в качестве входных данных для многослойных нейронных сетей.

В [52] для классификации записей из набора данных DARPA используется радиально-базисная нейронная сеть, в которой первые два слоя 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.

Генетические алгоритмы (ГА) основаны на имитации биологических принципов естественного отбора и предназначены для решения задач оптимизации [53]. Работа ГА начинается с создания начальной популяции индивидуумов. Каждый представитель популяции задается в виде набора генов (хромосом), представляющих собой символьные или бинарные последовательности (строки) и подвергающихся преобразованиям в процессе эволюции. Новое потомство генерируется при помощи операторов скрещивания и мутации. Эти операторы производят рекомбинацию хромосом и изменение структуры потомков. Для каждой особи нового потомства вычисляется значение приспособленности, которое характеризует показатель эффективности решения данной задачи.

Как правило, ГА применяются в совокупности с другими моделями классификации данных: деревьями решений, элементами нечеткой логики, нейронными сетями и т.д.

В [54] генетическое программирование применяется для создания новых правил распознавания образцов соединений в базе данных DARPA. Обучающая выборка содержит 8 классов атак, тестовое множество состоит из 10000 записей, описывающих 10 классов атак. Каждое правило представляется в виде древовидной структуры. В процессе выполнения операторов скрещивания или мутации заменяется отдельный узел этого дерева или целое поддерево.

В [55] ГА используются для создания начальных популяций нейронных сетей. Предлагается кодировать информацию о весовых коэффициентах и архитектуре нейросети как двоичную последовательность. По завершении работы ГА создается группа нейронных сетей с наиболее выигрышной структурой связи нейронов, количеством скрытых слоев и начальной настройкой весов.

В [56] применяется *нечеткая логика* совместно с ГА. Каждое правило задается четырьмя параметрами a, b, c, d $(a < b < c < d)$, которые кодируются как битовая последовательность и выступают в роли начальной популяции на входе ГА. Функция уверенности задается кусочно-линейной функцией, которая на интервале (a, b) принимает значения из $(0, 1)$, на интервале $[b, c]$ имеет значение 1 и на интервале (c, d) принимает значения, линейно убывающие от 1 до 0, в остальных случаях значение функции равно 0. Для каждого параметра соединения создается отдельное правило, подвергающееся улучшениям в процессе работы ГА. Если сумма значений функции уверенности по всем параметрам соединения превышает значение заданного порога, то соединение считается аномальным, иначе соединение классифи-

цируется как нормальное. Недостатком алгоритма является эвристическое задание величины порога.

В [57] для распознавания шаблонов легитимного сетевого трафика и образцов аномальных соединений используются правила классификации вида $if\ \langle condition\rangle\ then\ \langle act\rangle$, где $\langle condition\rangle$ — условие, $\langle act\rangle$ — действие. Посылка правила включала девять атрибутов набора данных DARPA, которые кодировались в виде строки из 57 целочисленных значений. Для получения новых правил классификации применялись операторы скрещивания и мутации.

В [58] для генерации правил экспертной системы применяются ГА и деревья решений. Для классификации соединений использовались 5 атрибутов: IP-адреса отправителя и получателя, их порты и тип протокола.

В [59] ГА используются для генерации правил системы обнаружения вторжений Snort на основе данных KDD Cup 99 [60]. Результаты экспериментов доказывают увеличение эффективности обнаружения шаблонов атак и снижение используемых вычислительных ресурсов.

Работа [61] посвящена разработке классификаторов на основе формальных грамматик, описанных с помощью форм Бэкуса-Наура. Авторы приводят пример, в котором каждое правило классификации представляется как вложенная цепочка условных операторов, закодированная последовательностью из 8-битовых значений (кодонов). ГА используется для генерации геномов, состоящих из переменного количества генов. Результатом работы ГА является программа с наибольшим значением функции приспособленности. Для классификации сетевых соединений используется ГА, генерирующий SQL-запросы к базе данных с записями KDD-99.

Вычислительные *иммунные системы* являются прототипом иммунной системы человека, построенным на основных принципах ее работы. Среди основных механизмов функционирования иммунной системы можно назвать создание и обучение иммунных детекторов, уничтожение детекторов, вызывающих ложные срабатывания, ответную реакцию на чужеродные патогены.

Более подробное описание искусственных иммунных систем можно найти в [62]. Первой моделью иммунной системы можно считать сетевую модель, предложенную английским физиологом Н.К. Ерне [63] в середине 70-х гг. 20 века. Данная модель построена на теории иммунной сети, состоящей из взаимосвязанных В-клеток для распознавания внешних антигенов. Согласно этой теории иммунная система представляет собой регулируемую сеть молекул и клеток, способных распознавать друг друга даже в условиях отсутствия антигена.

Теория основана на предположении, что различные клоны лимфоцитов не изолированы друг от друга, а поддерживают связь путем взаимодействия между своими рецепторами и антителами. В свою очередь антитела обладают набором специфических антигенных детерминант, называемых идиотопами. Поэтому такие структуры часто называют идиотипическими сетями [64].

Наиболее распространенными алгоритмами обучения являются отрицательный отбор и клональная селекция. Алгоритм отрицательного отбора [65] имитирует процесс созревания Т-клеток внутри тимуса и построен на основе принципов распознавания своего и чужого в системе иммунитета. Главной целью алгоритма является генерация такого набора детекторов, которые не совпадают ни с одним антителом организма. На первой стадии происходит случайное создание Т-клеток. На следующей стадии отсеиваются те клетки, которые реагируют на собственные антитела организма. Тем самым, остаются только те детекторы, которые могут обнаруживать только внешние антигены.

Алгоритм клональной селекции является эволюционным алгоритмом и применяется для решения задач оптимизации. Ключевым понятием данного алгоритма является свойство аффинности, характеризующее близость результата к оптимальному значению. На каждом шаге алгоритма для группы детекторов оптимизируется значение приспособленности [66].

В [67] рассматривают 3 способа генерации антител: положительная селекция, случайная генерация антител и отрицательный отбор.

Первый подход предполагает, что информация о легальном трафике напрямую используется для создания иммунных детекторов. Количество антител равно количеству элементов, описывающих легальный сетевой трафик. Этот метод прост и эффективен в обнаружении аномалий, но увеличение числа детекторов может привести к увеличению вычислительных затрат для обнаружения аномалий.

При случайной генерации антител информация о легальном трафике используется только как тестовое множество для построения популяции детекторов, которые создаются случайным способом. Если расстояние между произвольно созданным кандидатом в иммунные детекторы и одним из представителей легального трафика меньше некоторого порога, то первый включается в набор антител по распознаванию аномалий в сети.

Отрицательный отбор предлагает рассматривать антитела как правила следующей формы:

$$R^k\text{: if } \mathrm{x}_1 \in [\min_1^k, \max_1^k] \wedge \ldots \wedge x_n \in [\min_n^k, \max_n^k] \text{ then anomaly,}$$

где R^k — k-ое правило, которое может быть интерпретировано как n-мерный гиперкуб с ребрами $\min_1^k$ и $\max_1^k$, а $\{x_1, \ldots, x_n\}$ — параметры подозрительного трафика (антигена).

В отличие от двух предыдущих подходов здесь антитела генерируются так, чтобы покрыть часть n-мерного пространства, не принадлежащего легальному трафику.

Авторы [68, 69] предлагают модель иммунной системы с жизненным циклом Т-лимфоцитов, в которой учитывался процесс их созревания в тимусе, а также активация, формирование клеток иммунной памяти через сигнал костимуляции и гибель иммунных клеток. Разработанная ими система LISYS (Lightweight Immune SYStem) предназначена для обнаружения вторжений в распределенной среде. Хотя эта система обладает рядом преимуществ, включая относительно небольшие вычислительные издержки, надежность и масштабируемость, авторы отмечают некоторые из недостатков. Среди них — невозможность обнаружения сетевых атак с применением протокола UDP и возможность обмануть систему путем проведения распределенных во времени атак типа медленного сканирования.

Работа [70] предоставляет обзор двухуровневой системы обнаружения вторжений, в которой совмещены преимущества иммунных систем и сетей Кохонена. На первом этапе происходит фильтрация признаков сетевых соединений с помощью иммунных детекторов, обученных по методу отрицательного отбора, тем самым отсеиваются те образцы, которые соответствуют нормальным соединениям. На втором этапе аномальные экземпляры обрабатываются самоорганизующимися картами и группируются в отдельные кластеры со схожими признаками.

В [71] также представлена двухуровневая модель, в которой для обнаружения аномалий применялись иммунные системы, а для обнаружения злоупотреблений использовались нейронные сети с предобработкой входных данных при помощи метода главных компонент.

Классификатор, основанный на *методе опорных векторов* (англ. SVM, support vector machine), применяется, как правило, для классификации элементов из двух линейно разделимых множеств. Суть алгоритма заключается в построении оптимальной гиперплоскости, которая задается линейной комбинацией нескольких опорных векторов из обучающей выборки. В зависимости от расположения элемента по отношению к этой плоскости принимается решение о принадлежности элемента к тому или иному классу. В случае линейной неразделимости этих множеств вводится либо условие, минимизирующее ошибку распознавания (штраф), либо применяются различные ядра (отображения) для перехода к спрямляющим пространствам (возможно, большей размерности, чем

исходное). Существуют различные типы ядер, например, линейное, полиномиальное или гауссовское. В принципе, данное правило классификации попадает под модель Маккаллока-Питтса для построения однослойного перцептрона. Существенное отличие заключается лишь в алгоритме настройки весов (более контролируемое обучение, однозначность и оптимальность решения).

В [72] приведен сравнительный анализ эффективности распознавания образцов данных DARPA 1998 с помощью метода опорных векторов и нейронных сетей с одним скрытым слоем.

Среди других методов вычислительного интеллекта стоит отметить *роевые алгоритмы*, которые моделируют поведение и взаимодействие биологических особей в соответствующих «колониях» или «стаях» [73].

7. Гибридные методы. Существо гибридных подходов заключается в реализации различных схем объединения базовых классификаторов, которое позволяет нивелировать недостатки в их функционировании по отдельности. Выходные значения базовых классификаторов рассматриваются как промежуточные результаты, которые являются вспомогательными при формировании решающего правила верхнеуровневыми классификаторами [74].

В работах [75, 76] представлены три классификатора: дерево решений, SVM и комбинация первых двух классификаторов. Работа гибридного классификатора состояла из двух фаз. Сперва тестовые данные подавались на вход решающих деревьев, которые генерировали узловую информацию. Затем тестовые данные вместе с узловой информацией обрабатывались SVM, который выдавал результат классификации. Ключевой идеей в использовании этого подхода являлось 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.

В [77] применяется коллектив из 3 нейронных сетей и SVM. Выходное значение гибридного классификатора представляет собой взвешенную сумму выходов от четырех классификаторов, где веса вычисляются посредством минимизации среднеквадратичной ошибки.

В [70] 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.

В [78-80] комбинируется аппарат иммунных систем и нейронных сетей. В качестве иммунных детекторов выбраны многослойные нейронные сети, которые генерируются при помощи метода клональной селекции. Эксперименты были проведены на наборе данных KDD Cup 99, они доказали высокую способность детекторов приспосабливаться к новым типам атак.

Другим гибридным решением к задаче обнаружения вторжений является комбинирование нескольких нейронных сетей в единый классификатор. Так, работа [81] посвящена применению метода SVM и радиально-базисных сетей для классификации записей из набора данных NSL-KDD. 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.

Авторы [77, 82] предлагают подавать выходные значения от нескольких нейронных сетей, обученных различными алгоритмами, на вход процедуры взвешенного голосования и голосования по большинству. На тестовой выборке, состоящей из 6890 образцов, достигнута точность классификации выше 99%.

Статья [83] описывает двухуровневую схему 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.

8. Предложения по использованию методов интеллектуального анализа данных в задачах обнаружения сетевых аномалий. В данном разделе рассмотрены несколько проблем, возникающих в процессе решения задачи обнаружения сетевых аномалий при помощи методов ИАД, предложены несколько рекомендаций, которые позволят разработчикам систем обнаружения атак задуматься о целесообразности применения таких подходов.

На данный момент ИАД применяется с большим успехом во многих областях: оптическом распознавании символов, обнаружении спама, идентификации биометрических показателей, построении рекомендательных сервисов. Но в то же время при использовании этой же технологии возникает ряд трудностей с обнаружением аномалий в компьютерных сетях. *С чем может быть связана особенность использования методов ИАД применительно к задаче обнаружения сетевых аномалий и как объяснить природу такого отличия от решения других задач на базе этой же технологии?* По определению обнаружение аномалий включает в себя детектирование ранее не встречавшихся атак, в то время как методы ИАД в контексте постановки такой задачи направлены всего лишь именно на поиск взаимосвязей и закономерностей в сетевом трафике, нахождении активности, похожей на ранее встречавшуюся в обучающей выборке [84]. Строго говоря, это не совсем одно и то же, что многие привыкли считать как способность методов ИАД к обнаружению новых типов атак. 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. Кроме того, трудно 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. Но все равно в коммерческих реализациях систем обнаружения атак главным образом используются методы на основе правил, с помощью которых можно вручную более тонко отслеживать и задавать варьирование параметров в наблюдаемой сети. Это объяснимо рядом их сильных сторон, среди которых можно назвать возможность обоснования, почему был зафиксирован тот или иной сигнал атаки в конкретный момент времени, а также возможность более простой настройки системы. На основании имеющегося набора правил и характеристик трафика можно выявить причину срабатывания этого правила. При использовании средств ИАД трудно сделать подобные выводы по отношению к детекторам аномалий. Во-первых, сам по себе такой детектор вследствие сложного алгоритма обучения и особенностей своего внутреннего устройства представляет собой черный ящик, функционирование которого скрыто от пользователя и разработчика. Во-вторых, если детектор с течением времени постоянно меняется, то это также усложняет задачу объяснения того факта, что сигнал тревоги, полученный от детектора, действительно является признаком атаки. Для упрощения этой задачи, возможно, потребуется дополнительно вводить процедуру сохранения промежуточ-

ных слепков, отражающих состояния детектора в фиксированные срезы времени, чтобы иметь возможность просмотра истории изменения его состояний с откатом к предыдущим слепкам. В противном случае, если детектор постоянно остается статичным, то это приводит к увеличению показателей ложных срабатываний и пропуска атак в будущем.

Следующей 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. *Как же отличать случаи, когда действительно легитимный трафик просто меняется, а когда начинается деятельность, свойственная атакующему?* Можно предположить, что смена характера трафика сопровождается резким и мощным всплеском сетевой активности от конкретного узла или подсети и существенными отклонениями наблюдаемых статистических параметров. Но здесь возникает обратная сторона такого отчасти ошибочного и поспешного рассуждения: могут возникать редкие варианты, когда при малых изменениях значений отслеживаемых признаков все равно проводится своеобразная атака. К примеру, атакующий может пытаться постепенно обучать детекторы ИАД, очень медленно приспосабливая их к все более вредоносной активности (т.н. «эффект кипяченой лягушки» [85]). После такой подстройки новые детекторы будут принимать ранее аномальные образцы как нормальные. Во избежание таких случаев нужно четко понимать, как отслеживаемые данные меняются с течением времени. Но, к сожалению, это, как правило, трудно осуществимо на практике. Поэтому можно обойтись тем требованием, чтобы детекторы расширяли свою область инспектирования очень медленно, кроме того, полезно задавать некоторые пороговые значения, дальше которых «расширяться» детекторам не дозволено.

Наконец, последний и, пожалуй, один из самых важных вопросов — *как выбирать признаки, характерные для нормального трафика и аномалий и пригодные для обучения моделей ИАД?* Как один из вариантов для решения этого вопроса необходимо 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. Другой способ построения признаков заключается в добавлении некоторой автоматизации к описанному выше подходу: сна-

чала в максимально возможном объеме описывается множество всех контролируемых атрибутов, а потом применяются методы корреляционного анализа для устранения компонент, а иногда и их линейных комбинаций, с близкой к нулю дисперсией. Оставшийся набор признаков может быть использован для обучения и проверки модели ИАД.

Итак, *какое применение методов ИАД видится к задаче обнаружения аномалий?* (1) Можно использовать эти методы для задания пороговых значений. (2) Можно использовать их для 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). (3) Можно использовать их совместно с сигнатурными методами на основе правил.

9. Заключение. В данной работе был проведен сравнительный анализ методов обнаружения и классификации сетевых атак. Рассмотренные подходы успешно используются научным сообществом при разработке систем обнаружения атак. Предложена классификационная схема рассмотренных подходов. Представлены предложения по использованию методов интеллектуального анализа данных в задачах обнаружения сетевых аномалий.

В лаборатории проблем компьютерной безопасности СПИИРАН в течение последних нескольких лет активно проводятся исследования в области обнаружения атак, в том числе в области использования многоагентных технологий для обнаружения вторжений [86-88], механизмов защиты от сетевых червей [89, 90], обнаружения вредоносных файлов [91, 92], использования методов вычислительного интеллекта и гибридных подходов для обнаружения сетевых атак [74, 93, 94].

Перспективными направлениями при проектировании систем обнаружения атак в настоящее время видится гибридизация подходов, которая позволила бы совмещать в себе преимущества сигнатурных и эвристических методов, а также использование технологий больших данных и проактивного мониторинга безопасности [95]. Одним из основных требований, предъявляемых к данным решениям, является обеспечение адаптивной и высоко масштабируемой аналитической обработки событий, обеспечивающей интеллектуальное управление большими объемами данных о безопасности в реальном или близком к реальному масштабе времени.

Литература

1. *Лукацкий А.В.* Обнаружение атак // СПб.: БХВ-Петербург. 2003. 608 с.
2. *Kumar S., Spafford E.H.* A Pattern Matching Model for Misuse Intrusion Detection // Proceedings of the 17th National Computer Security Conference, 1994. pp. 11–21.
3. *Ghorbani A.A., Lu W., Tavallaee M.* Network Intrusion Detection and Prevention: Concepts and Techniques // Springer Science & Business Media. 2009. 212 p.
4. *Шаньгин В.Ф.* Информационная безопасность компьютерных систем и сетей // М.: ИД «ФОРУМ»: ИНФРА-М. 2008. 416 с.
5. *Anderson J.P.* Computer Security Threat Monitoring and Surveillance // Technical report, Fort Washington, Pennsylvania. 1980.
6. *Denning D.E.* An Intrusion-Detection Model // IEEE Transactions on software engineering, 1987, vol. SE-13, Issue 2. pp. 222–232.
7. *Jyothsna V., Prasad V.V.R.* A Review of Anomaly Based Intrusion Detection Systems // International Journal of Computer Applications. 2011. vol. 28, no. 7. pp. 26–35.
8. *Baddar S.A.-H., Merlo A., Migliardi M.* Anomaly Detection in Computer Networks: A State-of-the-Art Review // Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications. 2014. vol. 5. no. 4. pp. 29–64.
9. *Gyanchandani M., Rana J.L., Yadav R.N.* Taxonomy of Anomaly Based Intrusion Detection System: A Review // International Journal of Scientific and Research Publications. 2012. vol. 2. Issue 12. pp. 1–13.
10. *Tsai C.F., Hsub Y.F., Linc C.Y., Lin W.Y.* Intrusion detection by machine learning: A review // Expert Systems with Applications. 2009. vol. 36. Issue 10. pp. 11994–12000.
11. *Wu S.X., Banzhaf W.* The Use of Computational Intelligence in Intrusion Detection Systems: A Review // Applied Soft Computing, 2010, vol. 10, Issue 1. pp. 1–35.
12. *Kabiri P., Ghorbani A.A.* Research on Intrusion Detection and Response: A Survey // International Journal of Network Security. 2005. vol. 1, no. 2. pp. 84–102.
13. *Debar H., Dacier M., Wespi A.* Towards a taxonomy of intrusion-detection systems // Computer Networks. 1999. vol. 31. Issue 8. pp. 805–822.
14. *Barford P., Plonka D.* Characteristics of Network Traffic Flow Anomalies // Proceedings of the 1st ACM SIGCOMM Workshop on Internet Measurement. 2001. pp. 69–73.
15. *Kim S.S., Reddy A.L.* Statistical techniques for detecting traffic anomalies through packet header data // IEEE/ACM Transactions on Networking (TON). 2008. vol. 16. Issue 3. pp. 562–575.
16. *Barford P., Kline J., Plonka D., Ron A.* A signal analysis of network traffic anomalies // Proceedings of the 2nd ACM SIGCOMM Workshop on Internet measurement. 2002. pp. 71–82.
17. *Brindasri S., Saravanan K.* Evaluation Of Network Intrusion Detection Using Markov Chain // International Journal on Cybernetics & Informatics (IJCI). 2014. vol. 3. no. 2. pp. 11–20.
18. *Ye N., Chen Q.* An Anomaly Detection Technique Based on a Chi-square Statistic for Detecting Intrusions into Information Systems // Quality and Reliability Engineering International. 2001. vol. 17. Issue 2. pp. 105–112.
19. *Brockwell P.J., Davis R.A.* Introduction to Time Series and Forecasting // Springer Science & Business Media. 2006. 434 p.
20. *Lee W., Xiang D.* Information-theoretic measures for anomaly detection // Security and Privacy. 2001. pp. 130–143.
21. *Gu Y., McCallum A., Towsley D.* Detecting Anomalies in Network Traffic Using Maximum Entropy Estimation // Proceedings of the 5th ACM SIGCOMM conference on Internet Measurement. 2005. pp. 32–32.
22. *Babaie T., Chawla S., Ardon S.* Network Traffic Decomposition for Anomaly Detection // URL: http://arxiv.org/pdf/1403.0157.pdf, 2014 (Дата обращения: 08.03.2016).

23. *Крылов В.В., Самохвалова С.С.* Теория телетрафика и ее приложения // СПб.: БХВ-Петербург. 2005. 288 с.
24. *Mazurek M., Dymora P.* Network anomaly detection based on the statistical self-similarity factor for HTTP protocol // Przeglad elektrotechniczny, ISSN. 2014. pp. 127–130.
25. *Lee K., Kim J., Kwon K.H., Han Y., Kim S.* DDoS attack detection method using cluster analysis // Expert Systems with Applications. 2008. vol. 34. Issue 3. pp. 1659–1665.
26. Snort. Open Source Intrusion Detection System // URL: https://www.snort.org/ (дата обращения: 22.03.2016).
27. Suricata. Open Source IDS/IPS/NSM engine // URL: http://suricata-ids.org/ (дата обращения: 22.03.2016).
28. *Ilgun K., Kemmerer R.A., Porras P.A.* State Transition Analysis: A Rule-Based Intrusion Detection Approach // IEEE Transactions on Software Engineering. 1995. vol. 21. Issue 3. pp. 181–199.
29. *Kumar S., Spafford E.H.* A software architecture to support misuse intrusion detection // Proceedings of the 18th National Information Security Conference. 1995. pp. 194–204.
30. *Zhu W., Zhou Q., Li P.* Intrusion detection based on model checking timed interval temporal logic // IEEE International Conference on Information Theory and Information Security (ICITIS). 2010. pp. 503–505.
31. *Kruegel C., Toth T.* Using Decision Trees to Improve Signature-Based Intrusion Detection // Recent Advances in Intrusion Detection. 2003. pp. 173–191.
32. DARPA Intrusion Detection Data Sets // URL: https://www.ll.mit.edu/ideval/data/ (дата обращения: 22.03.2016).
33. *Heckerman D.* A Tutorial on Learning with Bayesian Networks // Innovations in Bayesian Networks: Theory and Applications. 2008. vol. 156. pp. 33–82.
34. *Barbara D., Wu N., Jajodia S.* Detecting Novel Network Intrusions Using Bayes Estimators // Proceedings of the First SIAM International Conference on Data Mining. 2001. pp. 1–17.
35. *Mukkamala S., Sung A.H., Abraham A., Ramos V.* Intrusion Detection Systems Using Adaptive Regression Splines // Sixth International Conference on Enterprise Information Systems. 2006. pp. 211–218.
36. *Ranjan R., Sahoo G.* A new clustering approach for anomaly intrusion detection // International Journal of Data Mining & Knowledge Management Process (IJDKP). 2014. vol. 4. no. 2. pp. 29–38.
37. *Guan Y., Ghorbani A.A., Belacel N.* Y-means: a clustering method for intrusion detection // Canadian Conference on Electrical and Computer Engineering, 2003. vol. 2. pp. 1083–1086.
38. *Wang Y.* A multinomial logistic regression modeling approach for anomaly intrusion detection // Computers & Security. 2005. vol. 24. Issue 8. pp. 662–674.
39. *Sammany M., Sharawi M., El-Beltagy M., Saroit I.* Artificial Neural Networks Architecture for Intrusion Detection Systems and Classification of Attacks // The 5th international conference INFO2007. 2007. pp. 24–26.
40. *Moradi M., Zulkernine M.* A Neural Network Based System for Intrusion Detection and Classification of Attacks // Proceedings of the IEEE International Conference on Advances in Intelligent Systems-Theory and Applications. 2004.
41. *Selim S., Hashem M., Nazmy T.M.* Intrusion Detection using Multi-Stage Neural Network // International Journal of Computer Science and Information Security (IJCSIS). 2010. vol. 8. no. 4. pp. 14–20.
42. *Cannady J.* Artificial Neural Networks for Misuse Detection // Proceedings of the 21st National Information Systems Security Conference. 1998. pp. 368–381.

43. *Ryan J., Lin M.-J.* Intrusion Detection with Neural Networks // Advances in Neural Information Processing Systems. 1998. pp. 943–949.
44. *Tan K.* The Application of Neural Networks to UNIX Computer Security // Proceedings of the IEEE International Conference on Neural Networks. 1995. vol. 1. pp. 476–481.
45. *Sheth H., Shah B., Yagnik S.* A survey on RBF Neural Network for Intrusion Detection System // Int. Journal of Engineering Research and Applications. 2014. vol. 4. Issue 12. pp. 17–22.
46. *Gnosh A.K., Michael C., Schatz M.* A Real-Time Intrusion Detection System Based on Learning Program Behavior // Proceedings of the 3rd International Workshop on Recent Advances in Intrusion Detection (RAID '00). 2000. vol. 1907. pp. 93–109.
47. *Hoglund A.J., Hatonen K., Sorvari A.S.* A Computer Host-Based User Anomaly Detection System Using The Self-Organizing Map // Proceedings of the IEEE-INNS-ENNS International Joint Conference on Neural Networks. 2000. vol. 5. pp. 411–416.
48. *Wang W., Guan X., Zhang X., Yang L.* Profiling program behavior for anomaly intrusion detection based on the transition and frequency property of computer audit data // Computers & Security. 2006. vol. 25. Issue 7. pp. 539–550.
49. *Bivens A., Palagiri C., Smith R., Szymanski B., Embrechts M.* Network-Based Intrusion Detection Using Neural Networks // Intelligent Engineering Systems through Artificial Neural Networks. 2002. vol. 12. pp. 579–584.
50. *Cannady J., Mahaffey J.* The Application of Artificial Neural Networks to Misuse Detection: Initial Results // Proceedings of the 1st International Workshop on Recent Advances in Intrusion Detection. 1998.
51. *Jirapummin C., Wattanapongsakorn N., Kanthamanon P.* Hybrid Neural Networks for Intrusion Detection System // Proceedings of the 2002 International Technical Conference on Circuits, Systems, Computers and Communications. 2002. vol. 7. pp. 928–931.
52. *Horeis T.* Intrusion detection with neural networks – combination of self-organizing maps and radial basis function networks for human expert integration // URL: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.106.191&rep=rep1&type=pdf. 2003. (дата обращения: 22.03.2016).
53. *Pawar S.N.* Intrusion Detection in Computer Network using Genetic Algorithm Approach: A Survey // International Journal of Advances in Engineering & Technology. 2013. vol. 6. Issue 2. pp. 730–736.
54. *Lu W., Traore I.* Detecting New Forms of Network Intrusion Using Genetic Programming // Computational intelligence. 2004. vol. 20. no 3. pp. 475–494.
55. *Jiang H., Ruan J.* The Application of Genetic Neural Network in Network Intrusion Detection // Journal of computers. 2009. vol. 4. no. 12. pp. 1223–1230.
56. *Ireland E.* Intrusion Detection with Genetic Algorithms and Fuzzy Logic // UMM CSci senior seminar conference. 2013. pp. 1–6.
57. *Li W.* Using Genetic Algorithm for Network Intrusion Detection // Proceedings of the United States Department of Energy Cyber Security Group. 2004. pp. 1–8.
58. *Sinclair C., Pierce L., Matzner S.* An Application of Machine Learning to Network Intrusion Detection // Proceedings of the 15th Annual Computer Security Applications Conference. 1999. pp. 371–378.
59. *Dave M.H., Sharma S.D.* Improved Algorithm for Intrusion Detection Using Genetic Algorithm and SNORT // International Journal of Emerging Technology and Advanced Engineering. 2014. pp. 273–276.
60. KDD Cup 1999 Data. URL: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html (дата обращения: 22.03.2016).
61. *Wilson D., Kaur D.* Using Grammatical Evolution for Evolving Intrusion Detection Rules // Proceedings of the 5th WSEAS Int. Conf. on Circuits, Systems, Electronics, Control & Signal Processing. 2006. pp. 42–47.

62. *De Castro L.N., Von Zuben F.J.* Artificial Immune Systems: Part I - Basic Theory and Applications // Universidade Estadual de Campinas, Dezembro de, Technical Report, 1999. 95 p.
63. *Jerne N.* Towards a network theory of the immune system // Ann. Immunol. (Inst. Pasteur). 1974. pp. 373–389.
64. *Dasgupta D.* Advances in Artificial Immune Systems // IEEE computational intelligence magazine. 2006. vol. 1. Issue 4. pp. 40–49.
65. *Forrest S., Perelson A.S., Allen L., Cherukuri R.* Self-Nonself Discrimination in a Computer // Proceedings of IEEE symposium on research in security and privacy. 1994. pp. 202–212.
66. *Kim J., Bentley P.J.* The Artificial Immune System for Network Intrusion Detection: An Investigation of Clonal Selection with a Negative Selection Operator // Proceedings of the Congress on Evolutionary Computation. 2001. pp. 1244–1252.
67. *Seredinski F., Bourvy P.* Anomaly detection in TCP/IP networks using immune systems paradigm // Computer communications. 2007. vol. 30. pp. 740–749.
68. *Hofmeyr S.A., Forrest S.* Architecture for an Artificial Immune System // Journal of Evolutionary Computation. 2000. vol. 8. no. 4. pp. 443–473.
69. *Hofmeyr S.A.* An Immunological Model of Distributed Detection and its Application to Computer Security // PhD thesis. Department of Computer Sciences, University of New Mexico. 1999. 113 p.
70. *Powers S.T., He J.* A Hybrid Artificial Immune System and Self Organising Map for Network Intrusion Detection // Information Sciences. 2008. vol. 178. Issue 15. pp. 3024–3042.
71. *Zhou Y.P.* Hybrid Model Based on Artificial Immune System and PCA Neural Networks for Intrusion Detection // Asia-Pacific Conference on Information Processing. 2009. vol. 1. pp. 21–24.
72. *Chen W.H., Hsu S.H., Shen H.P.* Application of SVM and ANN for intrusion detection // Computers & Operations Research. 2005. vol. 32. Issue 10. pp. 2617–2634.
73. *Rozenberg G., Bäck T., Kok J.N.* Handbook of natural computing // Springer Publishing Company, Incorporated. 2011. 2104 p.
74. *Branitskiy A., Kotenko I.* Network attack detection based on combination of neural, immune and neuro-fuzzy classifiers // The 18th IEEE International Conference on Computational Science and Engineering (IEEE CSE2015). 2015. pp. 152–159.
75. *Peddabachigari S., Abraham A., Grosan C., Thomas J.* Modeling intrusion detection system using hybrid intelligent systems // Journal of Network and Computer Applications. 2007. vol. 30. Issue 1. pp. 114–132.
76. *Abraham A., Thomas J.* Distributed intrusion detection systems: a computational intelligence approach // Applications of Information Systems to Homeland Security and Defense. 2005. pp. 105–135.
77. *Mukkamala S., Sung A.H., Abraham A.* Intrusion detection using ensemble of soft computing paradigms // Intelligent systems design and applications. 2003. vol. 23. pp. 239–248.
78. *Vaitsekhovich L.* Intrusion Detection in TCP/IP Networks Using Immune Systems Paradigm and Neural Network Detectors // XI International PhD Workshop OWD. 2009. pp. 219–224.
79. *Komar M., Golovko V., Sachenko A., Bezobrazov S.* Development of Neural Network Immune Detectors for Computer Attacks Recognition and Classification // IEEE 7th Intern. Conf. on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS). 2013. vol. 2. pp. 665–668.
80. *Golovko V., Komar M., Sachenko A.* Principles of Neural Network Artificial Immune System Design to Detect Attacks on Computers // Intern. Conf. on Modern Problems

of Radio Engineering, Telecommunications and Computer Science (TCSET). 2010. p. 237.
81. *Govindarajan M., Chandrasekaran R.M.* Intrusion Detection Using an Ensemble of Classification Methods // Proc. of the World Congress on Engineering and Computer Science. 2012. vol. 1. pp. 459–464.
82. *Mukkamala S., Sung A.H., Abraham A.* Intrusion Detection Using an Esemble of Intelligent Paradigms // Journal of Network and Computer Applications. 2005. vol. 28. Issue 2. pp. 167–182.
83. *Toosi A.N., Kahani M.* A New Approach to Intrusion Detection Based on an Evolutionary Soft Computing Model Using Neuro-Fuzzy Classifiers // Computer Communications. 2007. vol. 30. Issue 10. pp. 2201–2212.
84. *Sommer R., Paxson V.* Outside the Closed World: On Using Machine Learning For Network Intrusion Detection // IEEE Symposium on Security and Privacy (SP). 2010. pp. 305–316.
85. *Chan-Tin E., Feldman D., Hopper N., Kim Y.* The Frog-Boiling Attack: Limitations of Anomaly Detection for Secure Network Coordinate Systems // Security and Privacy in Communication Networks. Springer Berlin Heidelberg. 2009. pp. 448–458.
86. *Котенко И.В., Карсаев О.И.* Использование многоагентных технологий для комплексной защиты информации в компьютерных сетях // Известия ТРТУ. 2001. № 4, С. 38–50.
87. *Gorodetsky V., Kotenko I., Karsayev O.* The Multi-agent Technologies for Computer Network Security: Attack Simulation, Intrusion Detection and Intrusion Detection Learning // The International Journal of Computer Systems Science & Engineering. 2003. no. 4. pp. 191–200.
88. *Котенко И.В.* Многоагентные технологии для анализа уязвимостей и обнаружения вторжений в компьютерных сетях // Новости искусственного интеллекта. 2004. № 1. С. 56–72.
89. *Котенко И.В., Воронцов В.В., Чечулин А.А., Уланов А.В.* Проактивные механизмы защиты от сетевых червей: подход, реализация и результаты экспериментов // Информационные технологии. 2009. № 1. С. 37–42.
90. *Котенко И.В., Нестерук Ф.Г., Чечулин А.А.* Комбинирование механизмов обнаружения сканирования в компьютерных сетях // Вопросы защиты информации. 2011. № 3. С. 30–34.
91. *Komashinskiy D., Kotenko I.* Malware Detection by Data Mining Techniques Based on Positionally Dependent Features // Proceedings of the 18th Euromicro International Conference on Parallel, Distributed and network-based Processing (PDP 2010). 2010. pp. 617–623.
92. *Комашинский Д.В., Котенко И.В.* Обнаружение вредоносных документов формата PDF на основе интеллектуального анализа данных // Проблемы информационной безопасности. Компьютерные системы. 2012. № 1. С. 19–35.
93. *Браницкий А.А., Котенко И.В.* Построение нейросетевой и иммуноклеточной системы обнаружения вторжений // Проблемы информационной безопасности. Компьютерные системы. 2015. № 4. С. 23–27.
94. *Браницкий А.А., Котенко И.В.* Обнаружение сетевых атак на основе комплексирования нейронных, иммунных и нейро-нечетких классификаторов // Информационно-управляющие системы. 2015. № 4. С. 69–77.
95. *Котенко И.В., Саенко И.Б.* К новому поколению систем мониторинга и управления безопасностью // Вестник Российской академии наук. 2014. Том 84. № 11. С. 993–1001.

References

1. Lukatsky A.V. *Obnaruzhenie atak* [Attack Detection]. SPb.: BHV-Petersburg. 2003. 608 p. (In Russ.).
2. Kumar S., Spafford E.H. A Pattern Matching Model for Misuse Intrusion Detection. Proceedings of the 17th National Computer Security Conference. 1994. pp. 11–21.
3. Ghorbani A.A., Lu W., Tavallaee M. Network Intrusion Detection and Prevention: Concepts and Techniques. Springer Science & Business Media. 2009. 212 p.
4. Shan'gin V.F. *Informatsionnaya bezopasnost' komputernikh system i setey* [Information security of computer systems and networks]. M.: Publisher «FORUM»: INFRA-M. 2008. 416 p. (In Russ.).
5. Anderson J.P. Computer Security Threat Monitoring and Surveillance. Technical report, Fort Washington, Pennsylvania. 1980.
6. Denning D.E. An Intrusion-Detection Model. *IEEE Transactions on software engineering*, 1987, vol. SE-13, Issue 2. pp. 222–232.
7. Jyothsna V., Prasad V.V.R. A Review of Anomaly Based Intrusion Detection Systems. *International Journal of Computer Applications*. 2011. vol. 28, no. 7. pp. 26–35.
8. Baddar S.A.-H., Merlo A., Migliardi M. Anomaly Detection in Computer Networks: A State-of-the-Art Review. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*. 2014. vol. 5. no. 4. pp. 29–64.
9. Gyanchandani M., Rana J.L., Yadav R.N. Taxonomy of Anomaly Based Intrusion Detection System: A Review. *International Journal of Scientific and Research Publications*. 2012. vol. 2. Issue 12. pp. 1–13.
10. Tsai C.F., Hsub Y.F., Linc C.Y., Lin W.Y. Intrusion detection by machine learning: A review. *Expert Systems with Applications*. 2009. vol. 36. Issue 10. pp. 11994–12000.
11. Wu S.X., Banzhaf W. The Use of Computational Intelligence in Intrusion Detection Systems: A Review. *Applied Soft Computing*, 2010, vol. 10, Issue 1. pp. 1–35.
12. Kabiri P., Ghorbani A.A. Research on Intrusion Detection and Response: A Survey. *International Journal of Network Security*. 2005. vol. 1, no. 2. pp. 84–102.
13. Debar H., Dacier M., Wespi A. Towards a taxonomy of intrusion-detection systems. *Computer Networks*. 1999. vol. 31. Issue 8. pp. 805–822.
14. Barford P., Plonka D. Characteristics of Network Traffic Flow Anomalies. Proceedings of the 1st ACM SIGCOMM Workshop on Internet Measurement. 2001. pp. 69–73.
15. Kim S.S., Reddy A.L. Statistical techniques for detecting traffic anomalies through packet header data. *IEEE/ACM TON*. 2008. vol. 16. Issue 3. pp. 562–575.
16. Barford P., Kline J., Plonka D., Ron A. A signal analysis of network traffic anomalies. Proceedings of the 2nd ACM SIGCOMM Workshop on Internet measurement. 2002. pp. 71–82.
17. Brindasri S., Saravanan K. Evaluation Of Network Intrusion Detection Using Markov Chain. *International Journal on Cybernetics & Informatics (IJCI)*. 2014. vol. 3. no. 2. pp. 11–20.
18. Ye N., Chen Q. An Anomaly Detection Technique Based on a Chi-square Statistic for Detecting Intrusions into Information Systems. *Quality and Reliability Engineering International*. 2001. vol. 17. Issue 2. pp. 105–112.
19. Brockwell P.J., Davis R.A. Introduction to Time Series and Forecasting. Springer Science & Business Media. 2006. 434 p.
20. Lee W., Xiang D. Information-theoretic measures for anomaly detection. *Security and Privacy*. 2001. pp. 130–143.
21. Gu Y., McCallum A., Towsley D. Detecting Anomalies in Network Traffic Using Maximum Entropy Estimation. Proceedings of the 5th ACM SIGCOMM conference on Internet Measurement. 2005. pp. 32–32.
22. Babaie T., Chawla S., Ardon S. Network Traffic Decomposition for Anomaly Detection. Available at: http://arxiv.org/pdf/1403.0157.pdf, 2014 (accessed: 08.03.2016).

23. Krylov V.V., Samokhvalova V.V. *Teoriya teletrafika i ee prilozheniya* [Teletraffic Theory and Its Applications]. SPb.: BHV-Petersburg. 2005. 288 p. (In Russ.).
24. Mazurek M., Dymora P. Network anomaly detection based on the statistical self-similarity factor for HTTP protocol. *Przeglad elektrotechniczny*. 2014. pp. 127–130.
25. Lee K., Kim J., Kwon K.H., Han Y., Kim S. DDoS attack detection method using cluster analysis. *Expert Systems with Applications*. 2008. vol. 34. Issue 3. pp. 1659–1665.
26. Snort. Open Source Intrusion Detection System. Available at: https://www.snort.org/ (accessed: 22.03.2016).
27. Suricata. Open Source IDS/IPS/NSM engine. Available at: http://suricata-ids.org/ (accessed: 22.03.2016).
28. Ilgun K., Kemmerer R.A., Porras P.A. State Transition Analysis: A Rule-Based Intrusion Detection Approach. *IEEE Transactions on Software Engineering*. 1995. vol. 21. Issue 3. pp. 181–199.
29. Kumar S., Spafford E.H. A software architecture to support misuse intrusion detection. Proceedings of the 18th National Information Security Conference. 1995. pp. 194–204.
30. Zhu W., Zhou Q., Li P. Intrusion detection based on model checking timed interval temporal logic. IEEE International Conference on Information Theory and Information Security (ICITIS). 2010. pp. 503–505.
31. Kruegel C., Toth T. Using Decision Trees to Improve Signature-Based Intrusion Detection. *Recent Advances in Intrusion Detection*. 2003. pp. 173–191.
32. DARPA Intrusion Detection Data Sets. Available at: https://www.ll.mit.edu/ideval/data/ (accessed: 22.03.2016).
33. Heckerman D. A Tutorial on Learning with Bayesian Networks. *Innovations in Bayesian Networks: Theory and Applications*. 2008. vol. 156. pp. 33–82.
34. Barbara D., Wu N., Jajodia S. Detecting Novel Network Intrusions Using Bayes Estimators. Proceedings of the First SIAM International Conference on Data Mining. 2001. pp. 1–17.
35. Mukkamala S., Sung A.H., Abraham A., Ramos V. Intrusion Detection Systems Using Adaptive Regression Splines. Sixth International Conference on Enterprise Information Systems. 2006. pp. 211–218.
36. Ranjan R., Sahoo G. A new clustering approach for anomaly intrusion detection. *International Journal of Data Mining & Knowledge Management Process (IJDKP)*. 2014. vol. 4. no. 2. pp. 29–38.
37. Guan Y., Ghorbani A.A., Belacel N. Y-means: a clustering method for intrusion detection. Canadian Conference on Electrical and Computer Engineering, 2003. vol. 2. pp. 1083–1086.
38. Wang Y. A multinomial logistic regression modeling approach for anomaly intrusion detection. *Computers & Security*. 2005. vol. 24. Issue 8. pp. 662–674.
39. Sammany M., Sharawi M., El-Beltagy M., Saroit I. Artificial Neural Networks Architecture for Intrusion Detection Systems and Classification of Attacks. The 5th international conference INFO2007. 2007. pp. 24–26.
40. Moradi M., Zulkernine M. A Neural Network Based System for Intrusion Detection and Classification of Attacks. Proceedings of the IEEE International Conference on Advances in Intelligent Systems-Theory and Applications. 2004.
41. Selim S., Hashem M., Nazmy T.M. Intrusion Detection using Multi-Stage Neural Network. *International Journal of Computer Science and Information Security (IJCSIS)*. 2010. vol. 8. no. 4. pp. 14–20.
42. Cannady J. Artificial Neural Networks for Misuse Detection. Proceedings of the 21st National Information Systems Security Conference. 1998. pp. 368–381.
43. Ryan J., Lin M.J. Intrusion Detection with Neural Networks. *Advances in Neural Information Processing Systems*. 1998. pp. 943–949.

44. Tan K. The Application of Neural Networks to UNIX Computer Security. Proceedings of the IEEE International Conference on Neural Networks. 1995. vol. 1. pp. 476–481.
45. Sheth H., Shah B., Yagnik S. A survey on RBF Neural Network for Intrusion Detection System. *Int. Journal of Engineering Research and Applications*. 2014. vol. 4. Issue 12. pp. 17–22.
46. Gnosh A.K., Michael C., Schatz M. A Real-Time Intrusion Detection System Based on Learning Program Behavior. Proceedings of the 3rd International Workshop on Recent Advances in Intrusion Detection (RAID '00). 2000. vol. 1907. pp. 93–109.
47. Hoglund A.J., Hatonen K., Sorvari A.S. A Computer Host-Based User Anomaly Detection System Using The Self-Organizing Map. Proceedings of the IEEE-INNS-ENNS International Joint Conference on Neural Networks. 2000. vol. 5. pp. 411–416.
48. Wang W., Guan X., Zhang X., Yang L. Profiling program behavior for anomaly intrusion detection based on the transition and frequency property of computer audit data. *Computers & Security*. 2006. vol. 25. Issue 7. pp. 539–550.
49. Bivens A., Palagiri C., Smith R., Szymanski B., Embrechts M. Network-Based Intrusion Detection Using Neural Networks. *Intelligent Engineering Systems through Artificial Neural Networks*. 2002. vol. 12. pp. 579–584.
50. Cannady J., Mahaffey J. The Application of Artificial Neural Networks to Misuse Detection: Initial Results. Proceedings of the 1st International Workshop on Recent Advances in Intrusion Detection. 1998.
51. Jirapummin C., Wattanapongsakorn N., Kanthamanon P. Hybrid Neural Networks for Intrusion Detection System. Proceedings of the 2002 International Technical Conference on Circuits, Systems, Computers and Communications. 2002. vol. 7. pp. 928–931.
52. Horeis T. Intrusion detection with neural networks – combination of self-organizing maps and radial basis function networks for human expert integration. Available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.106.191&rep=rep1&type=pdf. 2003. (accessed: 22.03.2016).
53. Pawar S.N. Intrusion Detection in Computer Network using Genetic Algorithm Approach: A Survey. *International Journal of Advances in Engineering & Technology*. 2013. vol. 6. Issue 2. pp. 730–736.
54. Lu W., Traore I. Detecting New Forms of Network Intrusion Using Genetic Programming. *Computational intelligence*. 2004. vol. 20. no 3. pp. 475–494.
55. Jiang H., Ruan J. The Application of Genetic Neural Network in Network Intrusion Detection. *Journal of computers*. 2009. vol. 4. no. 12. pp. 1223–1230.
56. Ireland E. Intrusion Detection with Genetic Algorithms and Fuzzy Logic. UMM CSci senior seminar conference. 2013. pp. 1–6.
57. Li W. Using Genetic Algorithm for Network Intrusion Detection. Proceedings of the United States Department of Energy Cyber Security Group. 2004. pp. 1–8.
58. Sinclair C., Pierce L., Matzner S. An Application of Machine Learning to Network Intrusion Detection. Proceedings of the 15th Annual Computer Security Applications Conference. 1999. pp. 371–378.
59. Dave M.H., Sharma S.D. Improved Algorithm for Intrusion Detection Using Genetic Algorithm and SNORT. *International Journal of Emerging Technology and Advanced Engineering*. 2014. pp. 273–276.
60. KDD Cup 1999 Data. Available at: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html (accessed: 22.03.2016).
61. Wilson D., Kaur D. Using Grammatical Evolution for Evolving Intrusion Detection Rules. Proceedings of the 5th WSEAS Int. Conf. on Circuits, Systems, Electronics, Control & Signal Processing. 2006. pp. 42–47.
62. De Castro L.N., Von Zuben F.J. Artificial Immune Systems: Part I - Basic Theory and Applications. Universidade Estadual de Campinas, Dezembro de, Technical Report, 1999. 95 p.

63. Jerne N. Towards a network theory of the immune system. Ann. Immunol. (Inst. Pasteur). 1974. pp. 373–389.
64. Dasgupta D. Advances in Artificial Immune Systems. *IEEE computational intelligence magazine*. 2006. vol. 1. Issue 4. pp. 40–49.
65. Forrest S., Perelson A.S., Allen L., Cherukuri R. Self-Nonself Discrimination in a Computer. Proceedings of IEEE symposium on research in security and privacy. 1994. pp. 202–212.
66. Kim J., Bentley P.J. The Artificial Immune System for Network Intrusion Detection: An Investigation of Clonal Selection with a Negative Selection Operator. Proceedings of the Congress on Evolutionary Computation. 2001. pp. 1244–1252.
67. Seredinski F., Bourvy P. Anomaly detection in TCP/IP networks using immune systems paradigm. *Computer communications*. 2007. vol. 30. pp. 740–749.
68. Hofmeyr S.A., Forrest S. Architecture for an Artificial Immune System. *Journal of Evolutionary Computation*. 2000. vol. 8. no. 4. pp. 443–473.
69. Hofmeyr S.A. An Immunological Model of Distributed Detection and its Application to Computer Security. PhD thesis. Department of Computer Sciences, University of New Mexico. 1999. 113 p.
70. Powers S.T., He J. A Hybrid Artificial Immune System and Self Organising Map for Network Intrusion Detection. *Information Sciences*. 2008. vol. 178. Issue 15. pp. 3024–3042.
71. Zhou Y.P. Hybrid Model Based on Artificial Immune System and PCA Neural Networks for Intrusion Detection. Asia-Pacific Conference on Information Processing. 2009. vol. 1. pp. 21–24.
72. Chen W.H., Hsu S.H., Shen H.P. Application of SVM and ANN for intrusion detection. *Computers & Operations Research*. 2005. vol. 32. Issue 10. pp. 2617–2634.
73. Rozenberg G., Bäck T., Kok J.N. Handbook of natural computing. Springer Publishing Company, Incorporated. 2011. 2104 p.
74. Branitskiy A., Kotenko I. Network attack detection based on combination of neural, immune and neuro-fuzzy classifiers. The 18th IEEE International Conference on Computational Science and Engineering (IEEE CSE2015). 2015. pp. 152–159.
75. Peddabachigari S., Abraham A., Grosan C., Thomas J. Modeling intrusion detection system using hybrid intelligent systems. *Journal of Network and Computer Applications*. 2007. vol. 30. Issue 1. pp. 114–132.
76. Abraham A., Thomas J. Distributed intrusion detection systems: a computational intelligence approach. *Applications of Information Systems to Homeland Security and Defense*. 2005. pp. 105–135.
77. Mukkamala S., Sung A.H., Abraham A. Intrusion detection using ensemble of soft computing paradigms. *Intelligent systems design and applications*. 2003. vol. 23. pp. 239–248.
78. Vaitsekhovich L. Intrusion Detection in TCP/IP Networks Using Immune Systems Paradigm and Neural Network Detectors. XI International PhD Workshop OWD. 2009. pp. 219–224.
79. Komar M., Golovko V., Sachenko A., Bezobrazov S. Development of Neural Network Immune Detectors for Computer Attacks Recognition and Classification. IEEE 7th Intern. Conf. on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS). 2013. vol. 2. pp. 665–668.
80. Golovko V., Komar M., Sachenko A. Principles of Neural Network Artificial Immune System Design to Detect Attacks on Computers. Intern. Conf. on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET). 2010. p. 237.

81. Govindarajan M., Chandrasekaran R.M. Intrusion Detection Using an Ensemble of Classification Methods. Proc. of the World Congress on Engineering and Computer Science. 2012. vol. 1. pp. 459–464.
82. Mukkamala S., Sung A.H., Abraham A. Intrusion Detection Using an Esemble of Intelligent Paradigms. *Journal of Network and Computer Applications*. 2005. vol. 28. Issue 2. pp. 167–182.
83. Toosi A.N., Kahani M. A New Approach to Intrusion Detection Based on an Evolutionary Soft Computing Model Using Neuro-Fuzzy Classifiers. *Computer Communications*. 2007. vol. 30. Issue 10. pp. 2201–2212.
84. Sommer R., Paxson V. Outside the Closed World: On Using Machine Learning For Network Intrusion Detection. IEEE Symposium on Security and Privacy (SP). 2010. pp. 305–316.
85. Chan-Tin E., Feldman D., Hopper N., Kim Y. The Frog-Boiling Attack: Limitations of Anomaly Detection for Secure Network Coordinate Systems. *Security and Privacy in Communication Networks*. Springer Berlin Heidelberg. 2009. pp. 448–458.
86. Kotenko I.V., Karsayev O.I. [Using the multi-agent technology for comprehensive protection of information in computer networks]. *Izvestija TRTU – News TSURE*. 2001. no. 4. pp. 38–50. (In Russ.).
87. Gorodetsky V., Kotenko I., Karsayev O. The Multi-agent Technologies for Computer Network Security: Attack Simulation, Intrusion Detection and Intrusion Detection Learning. *The International Journal of Computer Systems Science & Engineering*. 2003. no. 4. pp. 191–200.
88. Kotenko I.V. [Multi-agent technology for the analysis of vulnerabilities and intrusion detection in computer networks]. *Novosti iskusstvennogo intellekta – News of artificial intelligence*. 2004. no. 1. pp. 56–72. (In Russ.).
89. Kotenko I.V., Vorontsov V.V., Chechulin A.A., Ulanov A.V. [Proactive security mechanisms against network worms: approach, implementation and results of the experiments]. *Informacionnye tehnologii – Information Technology*. 2009. no. 1. pp. 37–42. (In Russ.).
90. Kotenko I.V., Netsteruk P.G., Chechulin A.A. [Combining scanning detection mechanisms in computer networks]. *Voprosy zashhity informacii – The protection of information*. 2011. no. 3. pp. 30–34. (In Russ.).
91. Komashinskiy D., Kotenko I. Malware Detection by Data Mining Techniques Based on Positionally Dependent Features. Proceedings of the 18th Euromicro International Conference on Parallel, Distributed and network-based Processing (PDP 2010). 2010. pp. 617–623.
92. Komashinskiy D.V., Kotenko I.V. [Detection of malicious PDF documents on the basis of data mining]. *Problemy informacionnoj bezopasnosti. Komp'juternye sistemy – Problems of information security. Computer systems*. 2012. no. 1. pp. 19–35. (In Russ.).
93. Branitskiy A.A., Kotenko I.V. [Construction of neural network and immunokletochnoy intrusion detection system]. *Problemy informacionnoj bezopasnosti. Komp'juternye sistemy – Problems of information security. Computer systems*. 2015. no. 4. pp. 23–27. (In Russ.).
94. Branitskiy A.A., Kotenko I.V. [Hacker attack detection based on aggregation of neural, immune and neuro-fuzzy classifiers]. *Informacionno-upravljajushhie sistemy – Information and Control Systems*. 2015. vol. 4. pp. 69–77. (In Russ.).
95. Kotenko I.V., Saenko I.B. [To a new generation of security monitoring and control systems]. *Vestnik Rossijskoj akademii nauk – Bulletin of the Russian Academy of Sciences*. 2014. vol. 84. no. 11. pp. 993–1001. (In Russ.).

Браницкий Александр Александрович — младший научный сотрудник, Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук (СПИИРАН). Область научных

интересов: безопасность компьютерных сетей, искусственный интеллект, функциональное программирование. Число научных публикаций — 11. branitskiy@comsec.spb.ru, http://www.comsec.spb.ru; 14-я линия В.О., д. 39, Санкт-Петербург, 199178; р.т.: +7(812)328–7181, Факс: +7(812)328–4450.

Branitskiy Alexander Alexanderovich — junior researcher, laboratory of Computer Security Problems of the St. Petersburg Institute for Informatics and Automation of the Russian Academy of Science (SPIIRAS). Research interests: security of computer networks, artificial intelligence, functional programming. The number of publications — 11. branitskiy@comsec.spb.ru, http://www.comsec.spb.ru; 39, 14-th Line V.O., St. Petersburg, 199178, Russia; office phone: +7(812)328–7181, Fax: +7(812)328–4450.

Котенко Игорь Витальевич — д-р техн. наук, профессор, заведующий лабораторией проблем компьютерной безопасности, Федеральное государственное бюджетное учреждение науки Санкт-Петербургского института информатики и автоматизации Российской академии наук (СПИИРАН). Область научных интересов: безопасность компьютерных сетей, в том числе управление политиками безопасности, разграничение доступа, аутентификация, анализ защищенности, обнаружение компьютерных атак, межсетевые экраны, защита от вирусов и сетевых червей, анализ и верификация протоколов безопасности и систем защиты информации, защита программного обеспечения от взлома и управление цифровыми правами, технологии моделирования и визуализации для противодействия кибер–терроризму. Число научных публикаций — 450. ivkote@comsec.spb.ru, http://www.comsec.spb.ru; 14-я линия В.О., д. 39, Санкт-Петербург, 199178; р.т.: +7(812)328–2642, Факс: +7(812)328–4450.

Kotenko Igor Vitalievich — Ph.D., Dr. Sci., professor, head of computer security problems Laboratory, St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences (SPIIRAS). Research interests: computer network security, including security policy management, access control, authentication, network security analysis, intrusion detection, firewalls, deception systems, malware protection, verification of security systems, digital right management, modeling, simulation and visualization technologies for counteraction to cyber terrorism. The number of publications — 450. ivkote@comsec.spb.ru, http://www.comsec.spb.ru; 39, 14-th Line V.O., St. Petersburg, 199178, Russia; office phone: +7(812)328–2642, Fax: +7(812)328–4450.

Поддержка исследований. Работа выполнена при финансовой поддержке РФФИ (проекты №14-07-00697, 14-07-00417, 15-07-07451, 16-37-00338, 16-29-09482 офи_м), при частичной поддержке бюджетных тем № 0073-2015-0004 и 0073-2015-0007, а также гранта РНФ 15-11-30029 в СПИИРАН.

Acknowledgements. This research is supported by RFBR (projects No. 14-07-00697, 14-07-00417, 15-07-07451, 16-37-00338, 16-29-09482), in part by the budget (projects No. 0073-2015-0004 and 0073-2015-0007) and by the grant of RSF 15-11-30029 in SPIIRAS.

РЕФЕРАТ

Браницкий А.А., Котенко И.В. **Анализ и классификация методов обнаружения сетевых атак.**

Стремительное развитие компьютерных сетей и информационных технологий вызывает ряд проблем, связанных с безопасностью сетевых ресурсов, которые требуют новых подходов. В настоящее время вопросы построения систем обнаружения атак представляют собой актуальное направление в области сетевых технологий.

В работе проводится анализ известных методов для обнаружения и классификации сетевых атак, предлагается обобщенная схема классификации этих методов.

Дается анализ поведенческих методов, методов на основе знаний, методов машинного обучения и вычислительного интеллекта. Рассматриваются также работы, в которых представлены гибридные решения по комбинированию отдельных решателей.

SUMMARY

Branitskiy A.A., Kotenko I.V. **Analysis and Classification of Methods for Network Attack Detection.**

The rapid development of computer networks and information technologies raises a number of issues related to the security of network resources, which require new approaches. Currently, the problems of constructing attack detection systems represent the relevant trend in the field of network technologies.

We examine the known methods for detection and classification of network attacks and propose the generalized classification scheme of these methods.

The analysis of behavioral methods, knowledge-based methods, methods of machine learning and computational intelligence is given. We also consider the papers which contain hybrid solutions of combining the individual classifiers.