АНАЛИЗ МЕТОДОВ РАСПОЗНАВАНИЯ КОМПЬЮТЕРНЫХ АТАК

Добкач Л.Я.*

Ключевые слова: *обнаружение вторжений, поведенческие методы, методы на основе знаний, сигнатуры атак, деревья решений, искусственные нейронные сети, гибридные методы.*

Аннотация.

Цель статьи: *изучение существующих методов обнаружения вторжений с позиций их достоинств и недостатков, а также с учетом их классификации.*

Методы исследования: *компаративный анализ, статистический анализ, сигнатурный анализ, теория графов, байесовский метод.*

Результаты: *методы обнаружения вторжений можно условно разделить на четыре группы: поведенческие методы (подходят для поиска аномалий), методы на основе знаний (подходят для поиска злоупотреблений), методы интеллектуального анализа данных (подходят для обоих направлений поиска), причем последние разветвляются на методы машинного обучения и методы вычислительного интеллекта. Перспективной группой методов выступают гибридные методы, сочетающие в себе элементы различных «чистых» методов, и на основе соотнесения наиболее значимых недостатков разобранных методов предлагается гибридный метод, использующий преимущества как искусственных нейронных сетей, так и сигнатурных методов.*

DOI: 10.21681/1994-1404-2020-1-67-75

Введение

Информационные активы стали неотъемлемой частью современной жизни и, как следствие, представляют интерес для злоумышленников. Чтобы заполучить доступ к защищаемым сведениям, они пробуют осуществить атаку на систему, где хранятся нужные им данные. Чтобы верно разобрать проблему распознавания атак и найти лучший способ их пресечения, необходимо понять, что собой представляют компьютерные атаки, какие они бывают и к каким последствиям могут привести в случае успешного вторжения.

Существует множество различных классификаций разного уровня подробности и проработанности, из которых становится очевидным широкое разнообразие путей реализации угроз информационной безопасности. Так, в труде Питера Мелла «Компьютерные атаки: что это и как им противостоять»[1] классификация основывается на возможных действиях злоумышленника (к примеру, удаленное и локальное проникновение, отказы в обслуживании, опробование портов, анализ сетевого трафика). Но данная классификация почти не освещает такую важную характеристику любой атаки, как сегмент системы, подвергаемый злонамеренному воздействию.

Компания *Internet Security Systems* предлагает две классификационные нотации, одна из которых представляет более компактное представление версии Мелла из пяти типов атак, а вторая вводит ранжирование по степени риска, местоположению субъекта атаки, подвергаемому атаке программному обеспечению (ПО) и характеру действий («черные ходы», атаки типа «отказ в обслуживании» (*DoS и DDoS*), потенциально незащищенная операционная система, неавторизованный доступ). Здесь теряется цель атаки, а также ее последствия.

Все классификации так или иначе предлагают деление многообразия атак на несколько типов. Если их окажется мало, система обнаружения вторжений (СОВ) не сможет предложить конкретный сценарий действий, поскольку факт злонамеренного воздействия (в котором еще надо убедиться) не дает сам по себе ключ к пресечению такового. Обратная ситуация, когда типов так много, представляет собой скорее набор будто бы не связанных между собой частных случаев, нежели стандартный алгоритм реагирования на схожие по какому-то признаку вторжения.

«Золотой серединой» будет небольшое количество типов атак, которые позволят средству защиты информации и администратору информационной безопасности совершить определенные заранее действия за минимальное время и, таким образом, обеспечить защиту информационных активов.

[1] *См.:* Аграновский А. В., Хади Р. А. Новый подход к защите информации — системы обнаружения компьютерных угроз // Jet Info: Информ. бюл. 2007. 4(167). 24 с.

* ***Добкач Леонид Яковлевич,*** *аспирант Московского государственного технического университета им. Н. Э. Баумана, Российская Федерация, г. Москва.*

E-mail: dobkachleo@mail.ru

В качестве классификации разнообразных атак мы будем пользоваться совокупностью из 4 классов (удаленные атаки *R2L*, повышение полномочий *U2R*, отказы в обслуживании *DOS* и зондирующие атаки *Probe*), введенной в базе данных *KDD Cup* 1999. Каждый из этих классов имеет особенности, позволяющие обеспечить верное реагирование на атаку.

Но чтобы это сделать, ее необходимо распознать, изучить и проанализировать существующие методы обнаружения вторжений, а также предложить, исходя из сопоставления их преимуществ и недостатков, новый эффективный метод обнаружения вторжений.

Сформулируем задачи: установить классификационную схему методов выявления атак; сформировать метод распознавания атак по данной классификации; формализовать полученный метод.

Теоретическая значимость исследования заключается в выявлении эффективного метода распознавания атак и его формализации; практическая — в реализации метода в системе обнаружения вторжений, что позволит лучше выявлять атаки, а значит, и защищать информационные активы пользователей и предприятий.

1. Классификация методов распознавания атак

Утверждения об особенностях классификации компьютерных атак в равной мере применимы к классификации методов их распознавания, как и для любой сложной системы. Однако на этот раз справедливым, хотя и предварительным, будет разбиение на две пары подходов:

а) ***Сигнатурные и адаптивные (интеллектуальные) методы.***

Многие СОВ основаны на сличении текущих событий сетевого трафика с базой известных сигнатур или, в более общем случае, с правилами на их основе. Это безусловно гарантирует уверенность, что выделенное событие представляет именно злонамеренное действие, однако плохо распознает необычные атаки [1]. В качестве примеров можно выделить открытые системы обнаружения вторжений *Snort* и *Suricata* [2].

Адаптивные методы связаны с интеллектуальной обработкой или предобработкой событий и стремительно набирают популярность, но им присуща вероятностная природа. При обучении средства защиты информации можно установить точность распознавания, и она едва ли окажется равной 100%. Нивелирование этого недостатка представляется нам неотъемлемой частью поиска наилучшего метода распознавания атак ввиду возможности с помощью методов этой группы выявлять те атаки, которые будут пропущены сигнатурной системой обнаружения вторжений.

б) ***Методы обнаружения аномалий и злоупотреблений.***

Можно провести взаимосвязь между этой парой подходов и первой, но здесь во главу угла ставится совершенно иная природа методов. Начнем с того, что аномалии можно искать, когда сформирован профиль «нормального» функционирования системы, и отклонения от нормы фиксируются и выдаются за попытку вторжения [1].

Злоупотребления, напротив, предполагают знания о таких цепочках событий, которые ведут к эксплуатированию уязвимостей и другому вреду информационной системы. Тут можно провести явную связь с сигнатурными методами, хотя ими возможности распознавания атак не ограничиваются.

С позиции обнаружения аномалий или злоупотреблений оказываются общими методы интеллектуального анализа данных, такие как нейронные сети, деревья решений, генетические алгоритмы и др. Отличие лишь в том, что рассматривается по умолчанию как главное, а что — как цель для выявления [3]. Если сравнивать с вышеописанной парой подходов, данная пара дает больше вариаций методов выявления атак[2].

Забегая вперед, заметим, что неменьшую популярность набирают не чисто адаптивные методы, а комбинации различных подходов, т. е. там, где вероятность распознавания атак недостаточна для уверенного принятия решения, помогают более строгие правила из сигнатурных методов и им подобных.

2. Поведенческие методы

Важную роль в обнаружении аномалий играют поведенческие методы [1, 4]. К ним можно отнести вейвлет-анализ, спектральный, статистический анализ, анализ энтропии, фрактальный анализ[3] и др. Объединяет их сравнение параметров наблюдаемого поведения с нормальным профилем системы. Здесь присутствует вероятностный фактор, из-за которого СОВ не всегда реагирует только на аномалии. Повышение точности сопряжено со значительными временными затратами, хотя на этот фактор можно закрыть глаза, сочтя его за подготовку к работе. Гораздо хуже, если на этом этапе злоумышленник планомерно внесет злонамеренные действия в нормальный профиль системы, тогда средство защиты информации будет воспринимать аномалии как должное.

Кратко рассмотрим перечисленные выше поведенческие методы. Итак, начнем с ***вейвлет-анализа*** [5]. Основывается он, как подсказывает название, на вейвлет-преобразовании, что придает вес наиболее полезной информации. Для этого вычисляются коэффициенты, использующиеся в разложении исходного сигнала по базисным функциям. Сам же сигнал представляет, к примеру, интенсивность сетевого трафика. Достоинства «приоритизации» затеняются неоднозначностью

[2] См.: *Корниенко А. А., Слюсаренко И. М.* Системы и методы обнаружения вторжений: современное состояние и направления совершенствования // *CIT Forum*, 2009. 16 с.

[3] См.: *Басараб М. А., Строганов И. С.* Обнаружение аномалий в информационных процессах на основе мультифрактального анализа // Вопросы кибербезопасности. 2014. № 4 (7). С. 30—40.

выбора базисных функций, большой вычислительной сложностью при расчете коэффициентов разложения сигнала и правильным заданием размера скользящего окна, в котором ищется аномалия [3].

Недалеко от вейвлет-анализа отстоит спектральный анализ. Метод основан на предположении, что компоненты аномального трафика отличаются от компонентов обычного трафика. Главные компоненты должны отражать наибольшую изменчивость исходного процесса, остальные рассматриваются как составляющие шума. Тогда при изменении размерности исходного пространства признаков путем анализа ковариационной матрицы элементов исследуемого процесса, например, методом главных компонентов, можно выделить наиболее информативные составляющие этого процесса [3].

Статистический анализ — это целая группа методов, куда входят цепи Маркова, метод среднеквадратичных отклонений, анализ временных рядов, пороговый анализ и др. Их чаще всего применяют для поиска аномалий, ведь они способны учитывать изменения поведения пользователя и выявлять измененные атаки. В то же время следует верно выбирать контролируемые параметры, чтобы лучше отличать аномалии от нормального трафика, что, впрочем, не гарантирует избавления от ложноположительных срабатываний. Некоторым методам также присущи рост занимаемой памяти, «злонамеренное» переобучение, отсутствие стационарности (для временных рядов) и др.

Одна из разновидностей статистического анализа приводится в [6]. Исходя из распределения нулевых значений признаков базы данных *KDD Cup* 1999, выводится классификатор глубокого автокодировщика. Метод дает общую корректность в 87%, при этом точность распознавания *R2L*-атак и отклик на зондирующие атаки оставляют желать лучшего.

В теории информации важным понятием является энтропия. Она взята на вооружение в следующем рассматриваемом методе — ***анализе энтропии***. Атаки воспринимаются как точки, принадлежащие какому-то аномальному классу, для чего требуются заметные затраты памяти. Энтропия множества X вычисляется по формуле:

$$H(X) = -\sum_{x \in X} P(x) \cdot \log_2 P(x), \qquad (1)$$

где $P(x)$ — вероятность попадания события x в множество X.

Затраты памяти — вынужденная необходимость, обусловленная тем утверждением, что чем больше уникальных записей, тем равномернее их распределение относительно заданных классов множества X, отчего энтропия увеличивается [3].

3. Методы на основе знаний

Методы из данной группы чаще применяются для обнаружения злоупотреблений, т. е. на основе известных данных об атаках. Самыми распространенными среди них выступают ***сигнатурные методы***. По известным сигнатурам атак, составленных в виде регулярных выражений или правил на основе образца, проверяются текущие события, и становится точно известно, какое из них характеризует вторжение. Однако незнакомые сценарии вторжений и попросту неизвестные атаки останутся незамеченными. Помимо проблем с адаптивностью, подобным СОВ из-за больших баз сигнатур присуща низкая производительность [7].

Большей гибкостью обладают ***языки описания сценариев атак***, но из-за вычислительной сложности быстродействующими эти методы назвать нельзя. Эта проблема в меньшей степени серьезна для ***анализа систем состояний***, когда функционирование системы представляется в виде ориентированного графа с недопустимыми путями с опасными конечными состояниями[4]. Достаточно построить часть графа, чтобы выявить известные недопустимые пути, и это приводит к тому же недостатку, что и у сигнатурных методов — отсутствию адаптивности [3].

Еще один наглядный метод обнаружения злоупотреблений — анализ переходов состояний на основе раскрашенных ***сетей Петри***. Он реализован в СОВ *IDIOT* (англ. *Intrusion Detection In Our Time*). Сценарии вторжений преобразуются в шаблоны, с которыми сравниваются поступающие события безопасности. Достоинство метода — упреждение атаки, существенный недостаток — сложность реализации [3].

Система обнаружения вторжений *Snort* с открытым исходным кодом, считающаяся де-факто стандартом сигнатурных СОВ, также нередко называется ***экспертной системой***. Для таких реализаций характерны правила, которые называются продукционными. По сути, они представляют действие по условию, что приводит к быстродействию и точности работы. Однако перед началом применения необходимо набрать достаточно примеров, на основе которых и будут созданы искомые правила. Этот подход приводит к такому описанному выше недостатку, как адаптивность к неизвестным атакам [3].

Последним из методов обнаружения злоупотреблений рассмотрим ***метод проверки на модели***. Поскольку атака состоит из ряда отдельных операций, а также предпосылок, целей и ожидаемых результатов, можно сформировать поведенческие сценарии. От поведенческих методов он отличается, *во-первых*, стороной рассмотрения (злоупотребления вместо аномалий), а *во-вторых*, поиском подмножеств указанных сценариев атак. Другими словами, если в записях аудита обнаружится искомое подозрительное подмножество, так называемый антисипатор («предвосхититель») определяет, какие действия со стороны злоумышленника возможны следующими. Их планировщик более вни-

[4] См.: *Гамаюнов Д. Ю.* Обнаружение компьютерных атак на основе анализа поведения сетевых объектов : дисс. … канд. физ.-мат. наук: 05.13.11. М., 2007. 88 с.

мательно «высматривает» в записях аудита, предварительно преобразовав варианты поведения в системно-аудитозависимые выражения. Подозрения могут как оправдаться, так и быть опровергнуты, что влияет на вероятность наличия атаки в системе.

Благодаря тому, что «предвосхититель» начинает с обобщенных записей аудита, проверять все подряд необязательно — повышается быстродействие и точность. Планировщик обеспечивает независимость представления от формы данных аудита, т. е. универсальность. Однако все это хорошо лишь в теории, а практическая реализация сопряжена с проблемами отбора содержательных и точных количественных характеристик для разных частей графического представления модели и трудностями создания эффективного программного прототипа. Также метод нельзя назвать самостоятельным, не требующим применения других, он лучше работает вместе с подсистемой обнаружения аномалий [3].

4. Методы машинного обучения

Вышеперечисленные методы основаны, вне зависимости от стороны рассмотрения, на каких-то данных или знаниях, отчего большинству из них характерны значительные временные затраты, низкая производительность и (или) отсутствие гибкости, адаптивности [3]. Начиная с появления первого перцептрона, нейронные сети переживали то периоды подъема интереса к ним, то упадка. Сейчас мы наблюдаем очередную волну популярности, что подстегивается развитием вычислительных технологий. Методы машинного обучения и вычислительного интеллекта нашли применение и в области информационной безопасности.

Методы интеллектуального анализа могут в равной мере применяться для распознавания и аномалий, и злоупотреблений. Совершенно не важно, какой подход реализуется: искусственные нейронные сети (ИНС) и им подобные алгоритмы справятся с выявлением обоих типов подозрительной деятельности, обеспечивая бóльшую гибкость, нежели, к примеру, сигнатурные методы или экспертные системы [3].

Нейронные сети — лишь один из методов решения проблемы выявления атак. Наряду с ними существует еще множество других алгоритмов. Среди них: генетические и роевые алгоритмы, использование нечеткой логики, алгоритмы кластеризации, байесовские сети и метод, иммунные сети, деревья решений и др. Рассмотрим некоторые из них, и начнем с методов именно машинного обучения.

Метод ***деревьев решений*** может напомнить продукционные правила экспертных систем, но ему присуща адаптивность, повышение быстродействия, точность и верифицируемость[5]. Тем не менее, будучи вероятностным методом, стопроцентной точности обнаружения вторжений он не дает, причем чем меньше исходных данных для обучения, тем хуже результат [3]. Случайный лес, как ансамблевый алгоритм на основе деревьев решений, дает высокую точность (от 97%) распознавания атак и подтверждает свою эффективность в условиях, близких к реальным [8]. Деревья решений могут выступать в качестве метода обучения с учителем для обнаружения аномалий [9].

Следующими рассмотрим *байесовскую сеть* и ее частный случай — ***байесовский метод***. Они основаны на известной теореме Байеса, позволяя, таким образом, оценить апостериорную вероятность принадлежности события тому или иному классу. Для этого создается модель, где кодируются вероятностные отношения между событиями-переменными, а затем вычисляются условные вероятности их наступления. Байесовский метод иначе называется наивным байесовским классификатором, и его особенность — в предположении, что входные переменные независимы друг от друга. Из достоинств следует отметить возможность работы в режиме реального времени и обнаружение конкретных аномалий. Однако необходимо учитывать влияние измерений друг на друга, что сильно усложняет сам метод [3].

5. Методы вычислительного интеллекта

Именно к методам вычислительного интеллекта относится применение искусственных нейронных и иммунных сетей, генетических и роевых алгоритмов, опорных векторов и другие подходы к решению проблемы распознавания вторжений. Всем им, за исключением разве что метода опорных векторов, присуще «подглядывание» цепочки действий у живых существ (отдельного организма либо целой популяции) в переложении на язык математики.

Другими словами, машина реализует алгоритм, имитирующий явления живой природы, более гибкий в плане реакции на окружающий мир и при этом вычислительно более быстрый по сравнению с ней же. Так, ***нейронные сети*** способны по неполным данным делать выводы о новых объектах, в данном случае — относить их к тому или иному классу атак. При этом, как и живые существа, они могут ошибаться, а могут и верно догадываться. Все зависит от того, насколько хорошо они обучились и на какой обучающей выборке [10]. Возможность самообучения избавляет подобные системы от постоянного обновления сигнатур, уменьшает время реакции СОВ на аномалию сетевого трафика и позволяет увеличить объемы пропускаемого трафика, что ведет к обеспечению более высокого уровня защищенности информации [7].

Сети Кохонена [8], рекуррентные нейронные сети или сети глубокого доверия с применением классификатора с памятью способны эффективно распознавать

[5] См.: Брюховецкий А. А. Скатков А. В., Березенко П. О. Обнаружение уязвимостей в критических приложениях на основе решающих деревьев // Радиоэлектронные и компьютерные системы. № 5 (64). Харьков: Изд-во ХАИ, 2013. С. 18—23

низкоинтенсивные *DDoS*-атаки. Если обучить систему на нормальном трафике с небольшой примесью аномальных событий, что имитирует поведение реальных информационных систем, количество ошибок первого рода будет сведено до минимума [11].

Более сложным, хотя и похожим, методом выступают ***искусственные иммунные сети*** (ИИС), основанные на иммунной системе человека[6]. В основе их обучения лежат, как правило, такие алгоритмы, как отрицательный отбор и клональная селекция [3]. Первый отвечает за обнаружение только внешних антигенов, а значит, они способны отличить свои элементы от чужеродных. При этом генерируемые антитела рассматриваются как правила, описываемые формулой:

$$R^k: if\ x_1 \in \left[\min_1^k, \max_1^k\right] \wedge \ldots \wedge x_n \in \left[\min_n^k, \max_n^k\right]\ then\ anomaly, \quad (2)$$

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

Второй метод представляет собой эволюционный алгоритм для решения задач оптимизации[7]. В нем используется клональная селекция, а в качестве обучающей и тестовой выборок — данные базы данных *KDD Cup* 1999, что широко распространено в теоретических трудах. Результаты ИИС выявили достаточно высокую оценку распознавания, от 79,40% для *R*2L-атак (удаленных) до 93,42% для нормальных событий сетевого трафика.

Еще одним «биологическим» методом являются генетические алгоритмы (ГА). Если искусственные иммунные сети берут за основу иммунную систему человека, то ГА имитируют биологические принципы естественного отбора, математически представляя скрещивание и мутации в ходе эволюции генов. Нередко генетические алгоритмы применяют вместе с другими моделями классификации данных, например, с элементами нечеткой логики, рассмотренными выше деревьями решений, иммунными сетями и др. Эксперименты показали бóльшую эффективность обнаружения шаблонов атак и меньшее ресурсопотребление по сравнению с СОВ *Snort* [3].

Рассмотрим также метод опорных векторов (*SVM*, от англ. *support vector machine*), который часто применяется для классификации элементов из двух линейно разделимых множеств. Все множество разбивается гиперплоскостью, задаваемой линейной комбинацией нескольких опорных векторов из обучающей выборки. Если элемент оказался по одну сторону разделителя, значит, он в таком-то классе, иначе — в другом. Возможна линейная неразделимость на два множества, что влечет за собой условие для минимизации ошибки распознавания (так называемый штраф), либо же применяется линейное, полиномиальное или гауссовское ядро (отображение) для перехода к спрямляющим пространствам. Возникает сложность интерпретации параметров модели, а также невозможность калибровки вероятности попадания в определенный класс [3].

Для выявления удаленных атак и атак, направленных на повышение полномочий, можно взять за основу линейный дискриминант Фишера[8], а в качестве источника данных использовать базу данных *KDD Cup* 1999, из которой убрать признаки, наименее существенные для каждого отдельно взятого класса атак. Хотя для *U*2*R* результаты оказываются равны 99,9%, такой подход показал себя довольно посредственно (73,2% против 99,981% с помощью нейронных сетей на базе метода главных компонентов) в случае *R*2*L*.

Следует заметить, что *метод главных компонентов* часто используют для отбора значимых данных, но порой необходимо аннулировать корреляции между координатами, откуда берутся альтернативные способы избавления от избыточности [12]. Важность отбора признаков, наиболее полезных для распознавания образов, показана в [13], где сравнивались показатели точности выявления компьютерных атак без метода многофакторного анализа *ANOVA* и с ним. Улучшение стало наиболее заметным для класса *R*2*L*-атак (почти 22%), наименьшим — для нормальных событий сетевого трафика (0,49%).

Из приведенных характеристик следует вывод о неточности распознавания методами интеллектуального анализа. Такова цена за привнесение адаптивности в процесс распознавания атак. Многое упирается, как и в других методах, в затраты памяти (впрочем, в *радиально-базисных нейронных сетях* они не столь значительны для больших объемов входных данных обучающей выборки, как для ИНС *прямого распространения*) или в снижение производительности из-за вычислительной сложности алгоритма.

6. Гибридные методы

Решение проблемы с устранением недостатков различных методов лежит на поверхности: надо соединить два и более метода в один, гибридный, чтобы взять от обоих их преимущества, а недостатки оставить «оригинальным» алгоритмам [1]. Практическая реализация, безусловно, сложнее, однако можно достичь высоких показателей выявления вторжений путем нахождения наилучшего совмещения нескольких методов. Например, в [3] описан ансамбль из трех нейронных сетей, обученных разными алгоритмами, чьи выходные зна-

[6] См.: *Аграновский А.В., Хади Р.А.* Новый подход к защите информации — системы обнаружения компьютерных угроз // Jet Info: Информ. бюл. 2007. 4(167). 24 с.

[7] См.: *Брюховецкий А.А., Скатков А.В.* Адаптивная модель обнаружения вторжений в компьютерных сетях на основе искусственных иммунных систем // Электротехнические и компьютерные системы. № 12 (88). Одесса : ОНПУ, 2013. С. 102—111.

[8] См.: *Jeya P.G., Ravichandran M., Ravichandran C.S.* Efficient Classifier for R2L and U2R Attacks. International Journal of Computer Applications, vol. 45, 21, NY: Foundation of Computer Science, 2012, pp. 28-32.

чения подавали на вход процедуры взвешенного голосования и голосования по большинству (метод опорных векторов), и добились точности более 99%.

Приведенный пример как нельзя лучше подкрепляет утверждение о более высокой эффективности гибридных методов и подсказывает направление дальнейших изысканий. Теоретически мы допускаем, что ансамбль нейронных сетей, прошедших различное обучение, в совокупности с еще одной, «суммирующей» ИНС, обеспечат лучшие показатели как для выявления нормальных событий сетевого трафика, так и попыток вторжений.

Применение нейросетевого метода описано, например, в [14—16] для обнаружения низкоинтенсивных *DDoS*-атак на *web*-сервисы. В отличие от вышеприведенного классификатора с памятью [16], в качестве метода используется ансамбль одинаковых нейронных сетей для каждого сервиса (порта), величина окна задается в зависимости от данных, размерность уменьшают за счет кластеризации векторов самоорганизующейся картой, а вектора подают на вход многослойному перцептрону. Результаты даны с позиций ошибок первого и второго рода, которые не превышают 12% и 84%, соответственно, на одном и том же эксперименте с недостаточными данными, в основном же величина ошибки первого рода не превышает 6%, а второго рода — 10%. С учетом трудностей выявления низкоинтенсивных *DDoS*-атак, подобные результаты также подтверждают перспективность использования гибридных методов.

Не все «чистые» методы можно объединить так, чтобы получилась эффективная система защиты информации. Не имеет смысла использовать два и более метода, если их общие недостатки не компенсируются, а наоборот, усугубляются. Поэтому соберем все выделенные отрицательные стороны рассмотренных методов в табл. 1.

Таблица 1

Недостатки методов распознавания атак

Метод	Группы недостатков				
	Затраты времени	Затраты памяти	Сложность реализации	Нет адаптивности	Неточность (на известных данных)
1. Поведенческие методы					
Вейвлет-анализ	+		+		
Спектральный анализ	+		+		
Статистический анализ		+			+
Анализ энтропии		+			+
2. Методы на основе знаний					
Сигнатурные методы	+	+		+	
Языки описания сценариев атак	+		+		
Анализ систем состояний				+	
Сети Петри			+		
Экспертные системы		+		+	
Метод проверки на модели			+		
3. Методы машинного обучения					
Деревья решений					+
Байесовские сети			+		
Байесовский метод			+		
4. Методы вычислительного интеллекта					
Нейронные сети					+
Иммунные сети					+
Генетические алгоритмы	+		+		+
Метод опорных векторов			+		

В табл. 1 не учитываются некоторые специфические недостатки, такие, как, например, применимость метода опорных векторов только для двух классов. Также следует заметить, что приведенными методами их многообразие не ограничивается. Нейронные сети в совокупности с методами на основе знаний (допустим, сигнатурными методами) потенциально могут дать высокие результаты с позиции точности, так как ИНС способны обучаться на базе данных сигнатур известных атак и делать выводы о принадлежности незнакомых событий сетевого трафика к конкретному классу, не имея жесткой зависимости от базы сигнатур [17].

Ввиду приведенных выше примеров дополнительную точность могут придать ансамблевые структуры [3, 8, 15]. Однако чрезмерное употребление этого подхода может привести, напротив, к затратам как времени, так и памяти. В рамках задачи распознавания компьютерных атак необходимо снизить количество ошибок *второго рода* (пропуски цели), а также получить, по возможности, малое число ошибок *первого рода* (ложные тревоги).

С учетом изложенного теоретически эффективным гибридным методом представляется ансамбль нейронных сетей, не только обученных на множестве известных сигнатур различных событий сетевого трафика, но и учитывающих их непосредственно при принятии решения, что можно описать формулой:

$$K(x) = \begin{cases} \left[\dfrac{\sum_{i=1}^{n} \dfrac{T_i SK^2(x)}{P_i(x)}}{n}\right], SK(x) \neq 0 \\ \left[\dfrac{\sum_{i=1}^{n} T_i P_i(x)}{n}\right], SK(x) = 0 \end{cases} \quad (3)$$

где x — событие сетевого трафика; n — количество ИН; $K(x)$ — класс события x; T_i — точность i-й ИНС (уровень ложной тревоги); $P_i(x)$ — вероятный класс события x для i-й ИНС; $SK(x)$ — класс события x (если известна его сигнатура).

Пример с несколькими вариантами распределения значений класса (от 0 — для незнакомых событий и от 1 до 5 — для известных) приведен в табл. 2. Там же приведены результаты вычисления класса по формуле (3): округленные и приведенные с точностью до одного знака после запятой. Можно видеть, что в данном случае правила округления вынуждены отличаться от обычных, так как, например, 6 класса не существует, а 0 класс предназначен для незнакомых событий сетевого трафика.

Таблица 2

Теоретический эксперимент

$SK(x) \setminus T_i$	0,7	0,3	0,9	
1	4	3	2	1 (0,2)
3	2	2	2	3 (2,8)
0	3	4	1	1 (1,4)
5	5	1	4	5 (5,5)
3	1	2	5	3 (3,1)

Заключение

Таким образом, рассмотрено около двадцати существующих подходов, которые можно условно разделить на четыре группы, а также два направления поисков:

1. **Для поиска аномалий:**
1.1. Поведенческие методы.
1.2. Методы интеллектуального анализа данных.
2. **Для поиска злоупотреблений:**
2.1. Методы на основе знаний.
2.2. Методы интеллектуального анализа данных.

Методы интеллектуального анализа данных, в свою очередь, делятся на методы машинного обучения и *методы вычислительного интеллекта* (при этом, например, искусственные нейронные сети иногда относят к методам машинного обучения, поэтому представленное деление условно).

Также выделяются *гибридные методы*, представляющие интерес для перспективных исследований задачи распознавания компьютерных атак. К гибридным методам еще относятся *ансамблевые*, которые могут состоять как из нескольких реализаций одного подхода (так, в предлагаемом методе ансамбль состоит как минимум из трех ИНС, обученных на различных выборках образцов), так и различных подходов одной из вышеописанных групп.

Рассмотренные методы проанализированы с точки зрения преимуществ и недостатков. Последние были подвергнуты сравнительному анализу, на основе которого предложен *гибридный метод*, использующий адаптивность нейронных сетей и точность сигнатурных методов.

Теоретический эксперимент (см. табл. 2) удостоверяет целесообразность применения предложенного метода в несигнатурных системах обнаружения вторжений, что может обеспечить более высокий уровень защищенности информационных систем и сетей.

Рецензент: ***Цирлов Валентин Леонидович,*** *кандидат технических наук, доцент Московского государственного технического университета им. Н.Э. Баумана, г. Москва, Россия.*
E-mail: v.tsirlov@npo-echelon.ru

Литература

1. Ананьин Е. В., Кожевникова И. С., Лысенко А. В., Никишова А. В. Методы обнаружения аномалий и вторжений // Проблемы современной науки и образования. № 34 (76). Иваново : Олимп, 2016. С. 48—50.
2. Добкач Л. Я. Анализ эффективности систем обнаружения вторжений // Труды Всеросс. студ. конф. «Студенческая научная весна», посвященная 165-летию со дня рождения В. Г. Шухова» / Росмолодежь, МГТУ им. Н.Э. Баумана, СНТО им. Н.Е. Жуковского. М. : Изд. дом «Научная библиотека», 2018. С. 314—315.
3. Браницкий А. А., Котенко И. В. Анализ и классификация методов обнаружения сетевых атак // Труды СПИИРАН. № 2 (45). СПб. : ФГБУН «СПИИРАН», 2016. С. 207—244.
4. Вишневский А. С. Обманная система для выявления хакерских атак, основанная на анализе поведения посетителей веб-сайтов // Вопросы кибербезопасности. 2018. №3 (27). С. 54—62. DOI:10.21681/2311-3456-2018-3-54-62.
5. Микова С. Ю., Оладько В. С. Результат исследования алгоритмов выявления сетевых аномалий // Вопросы кибербезопасности. 2015. № 4(12). С. 38—41. DOI: 10.21681/2311-3456-2015-4-38-41.
6. Ieracitano C., Adeel A., Gogate M. [etc.] Statistical Analysis Driven Optimized Deep Learning System for Intrusion Detection. Proc. of the 9th International Conference on Brain Inspired Cognitive Systems (BICS 2018), Cham: Springer, 2018, pp. 759-769.
7. Кусакина Н. М. Методы анализа сетевого трафика как основа проектирования системы обнаружения сетевых атак // Труды XLI Междунар. науч.-прак. конф. "International Scientific Review of the Problems and Prospects of Modern Science and Education". Boston: Problems of Science, 2018. С. 28—31.
8. Кочетов Д. А., Лукащик Е.П. Нейросетевая технология обнаружения сетевых вторжений // Прикаспийский журнал: Управление и высокие технологии. 2018. № 2 (42). С. 104—112.
9. Шелухин О. И., Рябинин В. С., Фармаковский М. А. Обнаружение аномальных состояний компьютерных систем средствами интеллектуального анализа данных системных журналов // Вопросы кибербезопасности. 2018. № 2 (26). С. 33—43. DOI: 10.21681/2311-3456-2018-2-33-43.
10. Добкач Л. Я. Создание модуля распознавания атак для систем обнаружения вторжений // Труды Всеросс. студ. конф. «Студенческая научная весна», посвященная 85-летию Ю.А. Гагарина» / МГТУ им. Н.Э. Баумана, СНТО им. Н.Е. Жуковского. М. : Изд. дом «Научная библиотека», 2019. С. 36—37.
11. Чисоходова А. А., Сидоров И. Д. Модернизированный метод обнаружения низкоинтенсивных распределенных атак типа «отказ в обслуживании» // Успехи современной науки. 2017. Т. 1. С. 169—175.
12. Петрова В. И., Платонов В. В. Исследование методов сокращения размерности для обнаружения сетевых атак // Труды студ. науч. конф. «Информатика и кибернетика (COMCON-2016)» / Институт компьютерных наук и технологий. СПб. : СПбПУ им. Петра Великого, 2016. С. 210—213.
13. Марков Р. А., Бухтояров В. В., Попов А. М., Бухтоярова Н. А. Подход к выявлению инцидентов информационной безопасности // Научно-технический вестник Поволжья. 2016. № 1. С. 78—80.
14. Тарасов Я. В. Исследование применения нейронных сетей для обнаружения низкоинтенсивных DDoS-атак прикладного уровня // Вопросы кибербезопасности. 2017. № 5 (24). С. 23—29. DOI: 10.21681/2311-3456-2017-5-23-29.
15. Абрамов Е. С., Тарасов И.В. Применение комбинированного нейросетевого метода для обнаружения низкоинтенсивных DDoS-атак на web-сервисы // Инженерный вестник Дона. 2017. № 3 (46). С. 59.
16. Слесарчик К. Ф. Метод обнаружения низкоинтенсивных распределенных атак отказа в обслуживании со случайной динамикой характеристик фрагментации и периодичности // Вопросы кибербезопасности. 2018. № 1 (25). С. 19—27. DOI: 10.21681/2311-3456-2018-1-19-27.
17. Modorskiy A. M., Minzov A. S., Baronov O. R., Nevskiy A. Y. LAN Abnormalities Threat Detection: An Outlook and Applicability Analysis // Вопросы кибербезопасности. 2018. № 1(25). С. 11—18. DOI: 10.21681/2311-3456-2018-1-11-18.

AN ANALYSIS OF METHODS FOR IDENTIFYING COMPUTER ATTACKS

Leonid Dobkach, *Ph.D. student at the Bauman Moscow State Technical University, Russian Federation, Moscow.*
E-mail: dobkachleo@mail.ru

Keywords: *intrusion detection, behavioural methods, knowledge-based methods, attack signatures, decision trees, artificial neural networks, hybrid methods.*

Abstract.

Purpose of the paper: *studying the existing intrusion detection methods from the perspective of their advantages and drawbacks, as well as considering their classification.*

Methods of study: *comparative analysis, statistical analysis, signature-based analysis, graph theory, Bayesian method.*

Results obtained: *intrusion detection methods can be loosely divided into four groups: behavioural methods (suitable for searching anomalies), knowledge-based methods (suitable for searching abuses), and data mining methods (suitable for both search directions), the latter splitting into machine learning methods and computational intelligence methods. A promising group of such methods are hybrid methods combining elements of different 'pure' methods, and based on a comparison of the most significant weaknesses of analysed methods, a hybrid method using the strengths of artificial neural networks as well as of signature-based methods is put forth.*

References

1. Anan'in E. V., Kozhevnikova I. S., Lysenko A. V., Nikishova A. V. Metody obnaruzheniia anomalii i vtorzhenii. Problemy sovremennoi nauki i obrazovaniia, No. 34 (76), Ivanovo : Olimp, 2016, pp. 48-50.
2. Dobkach L. Ia. Analiz effektivnosti sistem obnaruzheniia vtorzhenii. Trudy Vseross. stud. konf. "Studencheskaia nauchnaia vesna", posviashchennaia 165-letiiu so dnia rozhdeniia V. G. Shukhova", Rosmolodezh', MGTU im. N.E. Baumana, SNTO im. N.E. Zhukovskogo, M. : Izd. dom "Nauchnaia biblioteka", 2018, pp. 314-315.
3. Branitskii A. A., Kotenko I. V. Analiz i klassifikatsiia metodov obnaruzheniia setevykh atak. Trudy SPIIRAN, No. 2 (45), SPb. : FGBUN "SPIIRAN", 2016, pp. 207-244.
4. Vishnevskii A. S. Obmannaia sistema dlia vyiavleniia khakerskikh atak, osnovannaia na analize povedeniia posetitelei veb-saitov. Voprosy kiberbezopasnosti, 2018, No.3 (27), pp. 54-62, DOI: 10.21681/2311-3456-2018-3-54-62.
5. Mikova S. Iu., Olad'ko V. S. Rezul'tat issledovaniia algoritmov vyiavleniia setevykh anomalii. Voprosy kiberbezopasnosti, 2015, No. 4(12), pp. 38-41, DOI: 10.21681/2311-3456-2015-4-38-41.
6. Ieracitano C., Adeel A., Gogate M. [etc.] Statistical Analysis Driven Optimized Deep Learning System for Intrusion Detection. Proc. of the 9th International Conference on Brain Inspired Cognitive Systems (BICS 2018), Cham: Springer, 2018, pp. 759-769.
7. Kusakina N. M. Metody analiza setevogo trafika kak osnova proektirovaniia sistemy obnaruzheniia setevykh atak. Trudy XLI Mezhdunar. nauch.-prak. konf. "International Scientific Review of the Problems and Prospects of Modern Science and Education", Boston: Problems of Science, 2018, pp. 28-31.
8. Kochetov D. A., Lukashchik E.P. Neirosetevaia tekhnologiia obnaruzheniia setevykh vtorzhenii. Prikaspiiskii zhurnal: Upravlenie i vysokie tekhnologii, 2018, No. 2 (42), pp. 104-112.
9. Shelukhin O. I., Riabinin V. S., Farmakovskii M. A. Obnaruzhenie anomal'nykh sostoianii komp'iuternykh sistem sredstvami intellektual'nogo analiza dannykh sistemnykh zhurnalov. Voprosy kiberbezopasnosti, 2018, No. 2 (26), pp. 33-43, DOI: 10.21681/2311-3456-2018-2-33-43.
10. Dobkach L. Ia. Sozdanie modulia raspoznavaniia atak dlia sistem obnaruzheniia vtorzhenii. Trudy Vseross. stud. konf. "Studencheskaia nauchnaia vesna", posviashchennaia 85-letiiu Iu.A. Gagarina", MGTU im. N.E. Baumana, SNTO im. N.E. Zhukovskogo, M. : Izd. dom "Nauchnaia biblioteka", 2019, pp. 36-37.
11. Chistokhodova A. A., Sidorov I. D. Modernizirovannyi metod obnaruzheniia nizkointensivnykh raspredelennykh atak tipa "otkaz v obsluzhivanii". Uspekhi sovremennoi nauki, 2017, t. 1, pp. 169-175.
12. Petrova V. I., Platonov V. V. Issledovanie metodov sokrashcheniia razmernosti dlia obnaruzheniia setevykh atak. Trudy stud. nauch. konf. "Informatika i kibernetika (COMCON-2016)", Institut komp'iuternykh nauk i tekhnologii, SPb. : SPbPU im. Petra Velikogo, 2016, pp. 210-213.
13. Markov R. A., Bukhtoiarov V. V., Popov A. M., Bukhtoiarova N. A. Podkhod k vyiavleniiu intsidentov informatsionnoi bezopasnosti. Nauchno-tekhnicheskii vestnik Povolzh'ia, 2016, No. 1, pp. 78-80.
14. arasov Ia. V. Issledovanie primeneniia neironnykh setei dlia obnaruzheniia nizkointensivnykh DDoS-atak prikladnogo urovnia. Voprosy kiberbezopasnosti, 2017, No. 5 (24), pp. 23-29, DOI: 10.21681/2311-3456-2017-5-23-29.
15. Abramov E. S., Tarasov I.V. Primenenie kombinirovannogo neirosetevogo metoda dlia obnaruzheniia nizkointensivnykh DDoS-atak na web-servisy. Inzhenernyi vestnik Dona, 2017, No. 3 (46), pp. 59.
16. Slesarchik K. F. Metod obnaruzheniia nizkointensivnykh raspredelennykh atak otkaza v obsluzhivanii so sluchainoi dinamikoi kharakteristik fragmentatsii i periodichnosti. Voprosy kiberbezopasnosti, 2018, No. 1 (25), pp. 19-27, DOI: 10.21681/2311-3456-2018-1-19-27.
17. Modorskiy A. M., Minzov A. S., Baronov O. R., Nevskiy A. Y. LAN Abnormalities Threat Detection: An Outlook and Applicability Analysis. Voprosy kiberbezopasnosti, 2018, No. 1(25), pp. 11-18, DOI: 10.21681/2311-3456-2018-1-11-18.