DOI 10.36622/VSTU.2022.25.4.014
УДК 004.056.5

МЕТОДЫ ИНТЕЛЛЕКТУАЛЬНОГО АНАЛИЗА ДАННЫХ, ПРИМЕНЯЕМЫЕ В ЗАДАЧЕ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

В.П. Лось, Д.Д. Маланьин

Развитие информационных технологий явилось причиной драматически возросшего числа атак на компоненты информационных систем, что, в свою очередь, сделало задачу обнаружения вторжений как никогда актуальной и важной. Применение методов интеллектуального анализа данных дает широкие возможности в различных областях науки и техники, в том числе для решения задач информационной безопасности. В рамках данной статьи предлагается классификация систем обнаружения вторжений по различным критериям. Приведен обзор популярных методов интеллектуального анализа данных, получивших широкое распространение в других областях науки, в разрезе применения к задаче обнаружения вторжений. Рассмотрен подход к решению задач обнаружения вторжений с применением рекуррентной нейронной сети.

Ключевые слова: информационная безопасность, система обнаружения вторжений, методы интеллектуального анализа данных.

Актуальность темы обнаружения вторжений связана, в первую очередь, со значительными достижениями в области интернет-технологий и симметричным ростом числа сетевых атак.

Так в статье SECURELIST [1] отмечается увеличение общего числа атак в период с I квартала 2021 года по I квартал 2022 года более, чем в 4,5 раза (рис. 1). В отчете компании Positive Technologies [2] отмечается увеличение числа атак на 14,8% по сравнению с IV кварталом 2021 года. Кроме того, в обоих материалах, а также в [3], отмечается значительный рост числа сетевых атак и, в частности, DDOS-атак.

Эксперты по кибербезопасности прогнозируют увеличение числа кибератак на российскую инфраструктуру в будущем году минимум на 50% [4], все это делает задачу обнаружения сетевых вторжений серьезной исследовательской проблемой. Несмотря на значительный прогресс и большой объем работ, все еще существует много возможностей для совершенствования технологий обнаружения и предотвращения сетевых вторжений, особого внимания заслуживают набирающие популярность в других областях методы интеллектуального анализа данных.

Любая комплексная система защиты информации, предназначенная для борьбы с различными векторами атак и состоит из множества уровней, первым из которых, обычно, считают элементы управления сетевой безопасностью.

В силу направленности работы далее речь пойдет именно о системах обнаружения вторжений (СОВ). СОВ позволяет обеспечить дополнительный уровень защиты компьютерных систем. Раннее обнаружение позволяет предотвратить вторжение и исключить его воздействие на системы.

Типовая архитектура СОВ включает в себя следующие компоненты:

— подсистему сбора информации, ответственную за первичный сбор информации посредством датчиков (сенсоров) с защищаемой системы;

— подсистему анализа, ответственную за обнаружение атак и вторжений, проводимых в отношении защищаемой системы;

— подсистему представления и обработки данных, которая обеспечивает интерфейс взаимодействия пользователя с СОВ, в первую очередь, для информирования о состоянии защищаемой системы.

Все СОВ могут быть классифицированы по большому числу признаков, основные из них представлены на рис. 2. Набор тех или

иных признаков у конкретно взятой СОВ применения. зависит в первую очередь от области ее

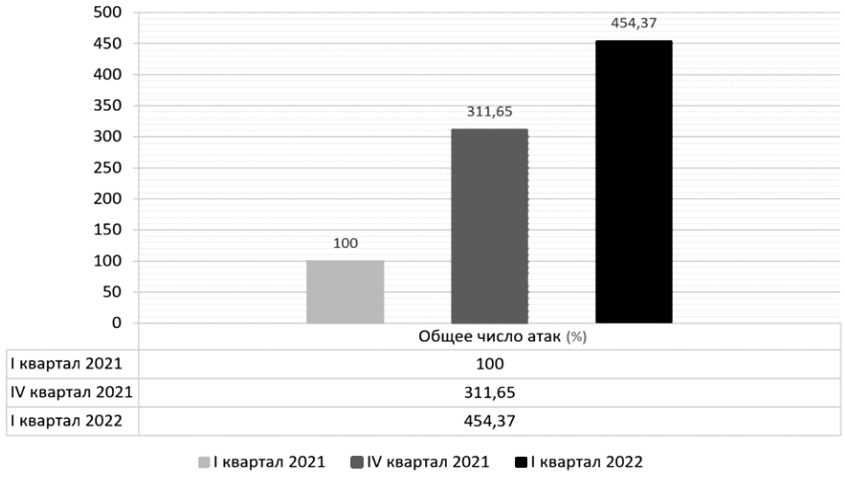

Рис. 1. Общее число атак по материалам «Лаборатории Касперского»

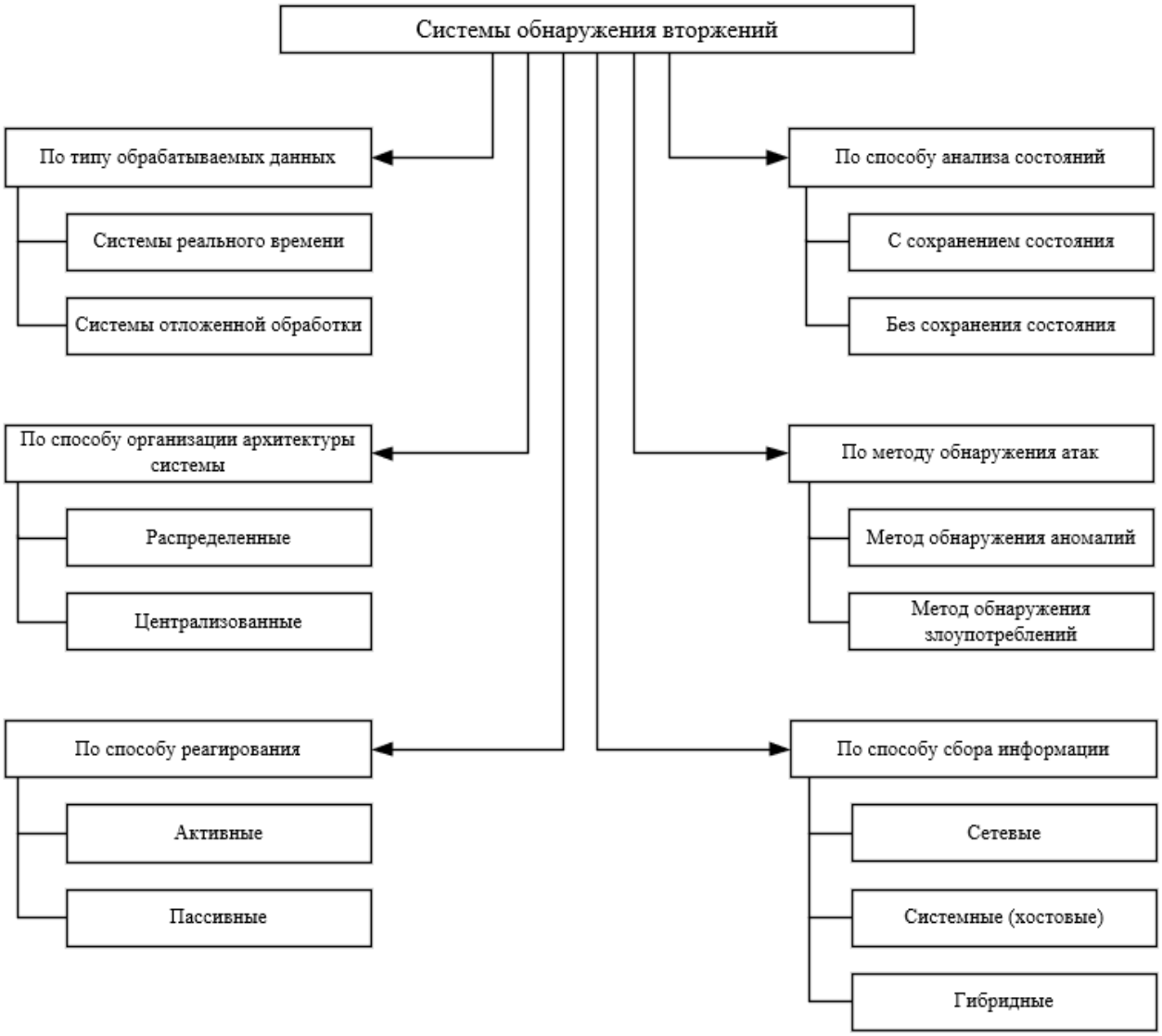

Рис. 2. Классификация СОВ по различным признакам

По способам выявления атак выделяют две группы СОВ:

— использующие методы обнаружения аномалий (anomaly detection), которые сравнивают агрегированный признаки, полученные из входных данных (набор сетевых пакетов, в общем случае – фрагментированных на уровне IP) с некоторым шаблоном нормального поведения объекта;

— использующие методы обнаружения злоупотреблений (misuse detection), которые, как и в случае с методами обнаружения аномалий, получают агрегированные признаки, которые сравниваются с набором правил, описывающих угрозы;

Оба способа имеют как свои достоинства, так и недостатки, так, например, проектирование шаблона нормального поведения для метода обнаружения аномалий является достаточно сложной задачей, более того, не всегда разрешимой, поскольку не каждое аномальное действие на практике является атакой, в то же время, создание исчерпывающей базы правил для систем, использующих метод обнаружения злоупотреблений представляется невозможным, поэтому в большинстве существующих СОВ применяются комплексные решения, основанные на синтезе вышеприведенных методов.

По способу реагирования выделают два вида СОВ:

— пассивные системы обнаружения вторжений – системы, осуществляющие сбор и анализ данных, а также журналирование с последующим информированием ответственных лиц или других систем о возникших угрозах;

— активные системы предотвращения вторжений – системы осуществляющие активные действия в случае обнаружения угрозы, например, посредством изменения конфигурации межсетевого экрана, блокировка источника угрозы, создания соответствующих списков маршрутизации и т.д.

Активную систему обнаружений вторжений также принято обозначать термином «система предотвращения вторжений» (СПВ) или же «система обнаружения и предотвращения вторжений» (СОиПВ)

По способу организации архитектуры системы обнаружения вторжений выделяют два вида СОВ:

— распределенные системы обнаружения вторжений – в подобного рода системах происходит распределение функции сбора информации между несколькими агентами (датчиками, установленными на узлах защищаемой системы);

— централизованные системы обнаружения вторжений – в подобных системах отсутствует распределение функции сбора информации о защищаемых системах.

Распределенные СОВ обладают как достоинствами, так и недостатками, так, например, к преимуществам системы можно отнести возможность сбора и последующего анализа большего объема информации, что, в свою очередь, позволяет обнаруживать более широкий спектр атак на защищаемую информационную систему. Наиболее существенными недостатками такой системы в сравнении с централизованными системами можно считать следующие:

— генерация значительно большего объема трафика, оказывающего дополнительную нагрузку на сеть;

— меньшая защищенность компонентов системы;

— необходимость в решении задачи по организации модуля принятия решений (возможны подходы одно- и многоступенчатого принятия решения о совершаемой атаке на защищаемую информационную систему).

По способу анализа состояний СОВ можно классифицировать на 2 группы:

— с сохранением состояния – система учитывает предыдущие состояния, а также учитывает при вынесении новых решений относительно анализируемых данных,

решения, который были вынесены системой ранее;

— без сохранения состояния – все события системой рассматриваются как независимые друг относительно друга.

По типу обрабатываемых данных СОВ разделяют на две категории:

— системы реального времени – системы, анализирующие поступающую информацию с подсистемы сбора информации в реальном времени;

— системы отложенной обработки событий – системы, анализирующие, объем данных, ранее записанного посредством журналов, предварительно захваченного трафика или же записанного подсистемой сбора информации.

Областью применения систем отложенной обработки событий может служить, например, проведение расследований инцидентов, произошедших в защищаемой системе или же снижение системных требований к СОВ, а систем реального времени, например, скорое обнаружение и реагирование на попытки реализации атак в отношении защищаемо информационной системы.

По способу сбора информации СОВ можно разделить на три группы:

— хостовые (системные) системы обнаружения вторжений (ХСОВ) анализируют сетевой трафик и системные настройки, такие как: вызовы программного обеспечения, локальную политику безопасности, аудит локальных журналов и многое другое. ХСОВ должна быть установлена на каждом компьютере и требует конфигурации, специфичной для этой операционной системы и программного обеспечения, что можно отнести к существенному недостатку данного подхода, так как большинство реальных сетей являются гетерогенными с точки зрения используемых в них программных компонентов. Примерами типов характеристик, которые может отслеживать ХСОВ на хосте, являются сетевой трафик (только для этого хоста), системные журналы, запущенные процессы, активность приложений, доступ к файлам и их изменение, а также изменения конфигурации системы и приложений. Системы подобного типа чаще всего развертываются на критически важных хостах, таких как общедоступные серверы и серверы, содержащие конфиденциальную информацию.

— сетевые системы обнаружения вторжений (ССОВ) — представляют собой один из наиболее распространенных видов СОВ, при котором анализируется сетевой трафик на всех уровнях сетевой модели OSI и принимаются решения о цели трафика, анализируя подозрительную активность. Подавляющее большинство ССОВ просты в своей интеграции в существующую сеть и позволяют осуществлять анализ трафика с нескольких детекторов одновременно.

Данный тип СОВ может идентифицировать множество различных типов событий, представляющих интерес. Чаще всего он развертывается на границе между сетями, например, вблизи пограничных брандмауэров или маршрутизаторов, серверов виртуальной частной сети (VPN), серверов удаленного доступа и беспроводных сетей.

На рис. 3 представлена типовая схема включения ССОВ, которая в общем случае состоит из:

— датчиков (или сенсоров);

— анализатора (или анализаторов), выполняющего анализ данных, собранных датчиками;

— хранилища выявленных событий и информации, необходимой для работы анализатора;

— консоли управления элементами ССОВ.

Основными элементами из перечисленных являются первые два.

— гибридные системы обнаружения вторжений – являются системами, обладающими признаками как ХСОВ, так и ССОВ.

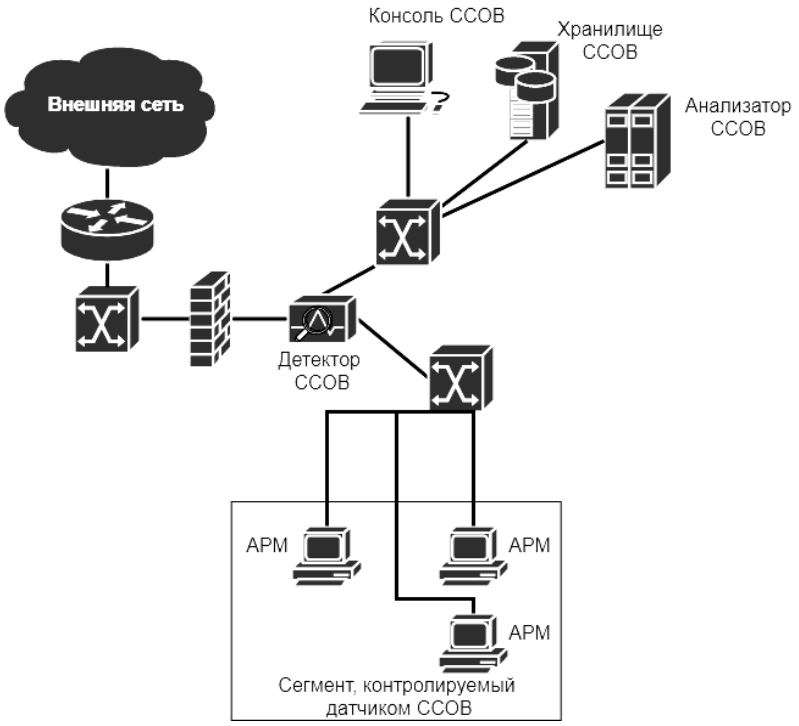

Рис. 3. Типовая схема включения ССОВ

Как было отмечено выше, современные СОВ могут обладать совершенно различным набором характеристик по приведенным классам, строго говоря, набор этих характеристик определяется в зависимости от сферы применения. Несмотря на это, можно выделить общее направление развития СОВ всех типов, а именно, повышение динамичности методов обнаружения за счет применения интеллектуальной модели, позволяющей учитывать постоянно меняющиеся методы совершения атак на защищаемую информационную систему.

Все большее внимание уделяется использованию методов интеллектуального анализа данных (ИАД), это подтверждают многочисленные работы в этой области, такие СОВ обеспечили более высокую скорость обнаружения, гибкость и адаптивность по сравнению с другими подходами (например, сигнатурным и статистическим анализом). ИАД представляет собой процесс, позволяющий проводить поиск и интерпретацию скрытых закономерностей из исходных данных, которые могут быть полезны при принятии решений в различных сферах человеческой деятельности. Одним из наиболее быстро развивающихся подклассов методов ИАД являются методы машинного обучения и их расширенное подмножество – методы искусственного интеллекта.

Рассмотрим некоторые популярные алгоритмы искусственного интеллекта, применяеме в СОВ, построенных на основе как методов обнаружения аномалий, так и методов обнаружения злоупотреблений.

Глубокие нейронные сети (ГНС) представляют собой многослойную нейронную сеть с прямой связью с некотором количеством скрытых слоев между входным и выходным слоями (рис. 4). Преимущество использования ГНС заключается в том, что они позволяют проводить точную классификацию для классов, в достаточном объеме представленных в обучающей выборке, кроме того, обладают высокой производительностью. ГНС способны извлекать функции высокого уровня из необработанных данных, используя подход многоуровневого персептрона.

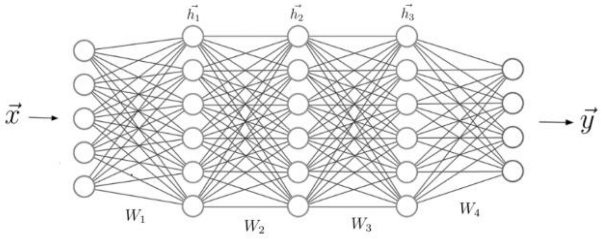

Рис. 4. Глубокая нейронная сеть, показаны входной, скрытые и выходной слои

Для ГНС, созданной для обнаружения вторжений в работе [5], было показано, что функция активации ReLU наиболее предпочтительна, нежели другие функции нелинейной активации.

Сверочные нейронные сети (СНС) позволяют обучать многослойные сети и позволяют работать с нелинейными и многомерными данными. Эти сети состоят из нейронов с обучаемыми весами и смещениями. Подобные модели предназначены для обработки данных, поступающих в виде нескольких массивов, и устраняют необходимость ручного извлечения признаков (рис. 5). СНС использует свертку как математическую операцию вместо умножения или скалярного произведения. Операция свертки включает настраиваемые гиперпараметры, такие как размерность фильтра, количество фильтров и шаги для создания результирующей матрицы.

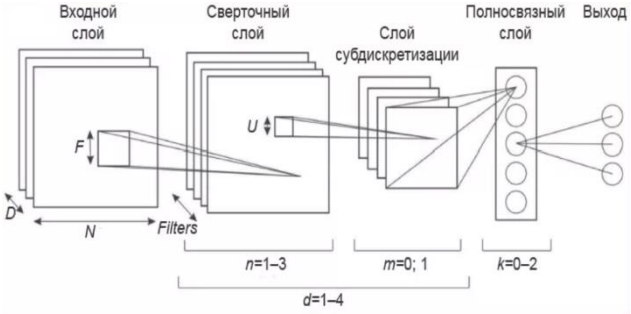

Рис. 5. Сверточная нейронная сеть

В работе [6] было предложено применение СНС для решения задачи обнаружения вторжений, путем преобразования одномерного массива сетевого потока в двумерный для передачи на вход СНС.

Автокодировщик — это категория искусственных нейронных сетей, в которых целевой выход сети обычно устанавливается равным ее входу. Автокодировщики позволяют использовать обучение без учителя, а используются в основном для уменьшения размерности набора данных. Алгоритм работы автокодировщика подразумевает сжатие входных данных в некоторое представление в скрытом пространстве, с последующим восстановлением данных из этого скрытого пространства (рис. 6).

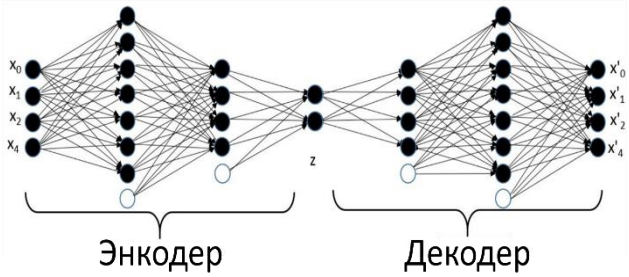

Рис. 6. Автокодировщик, показаны сжимающие слои – энкодер и восстанавливающие слои – декодер

Наиболее важными практическими приложениями автокодировщиков являются снижение уровня шума в данных и уменьшение размерности для визуализации данных.

Автокодировщики в задачах обнаружения вторжений, как правило, применяются в комплексе с другими алгоритмами, так, например, в [7] использовался автокодировщик в совокупности с методом опорных векторов, а в работе [8] – с использованием глубоких нейронных сетей.

Рекуррентные нейронные сети (РНС) являются расширением традиционных нейронных сетей и предназначены для моделирования данных последовательности. состоит из входного, рекуррентного и выходного блоков, где рекуррентные блоки считаются элементами памяти. В ходе принятия решения, каждая единица РНС опирается на свой текущий ввод и предшествующий вывод (рис. 7).

Для задач обнаружения вторжений РНС используется для контролируемой классификации и выделения признаков. Подход с использованием РНС для бинарной и многоклассовой классификации сетевых атак был предложен в работе [9].

Стоит отметить, что РНС обычно работает с последовательностями ограниченной длины, что ограничивает их применение при больших длинах последовательностей. Для обхода этого ограничения разработаны различные модификации РНС, например, GRU и LSTM [10].

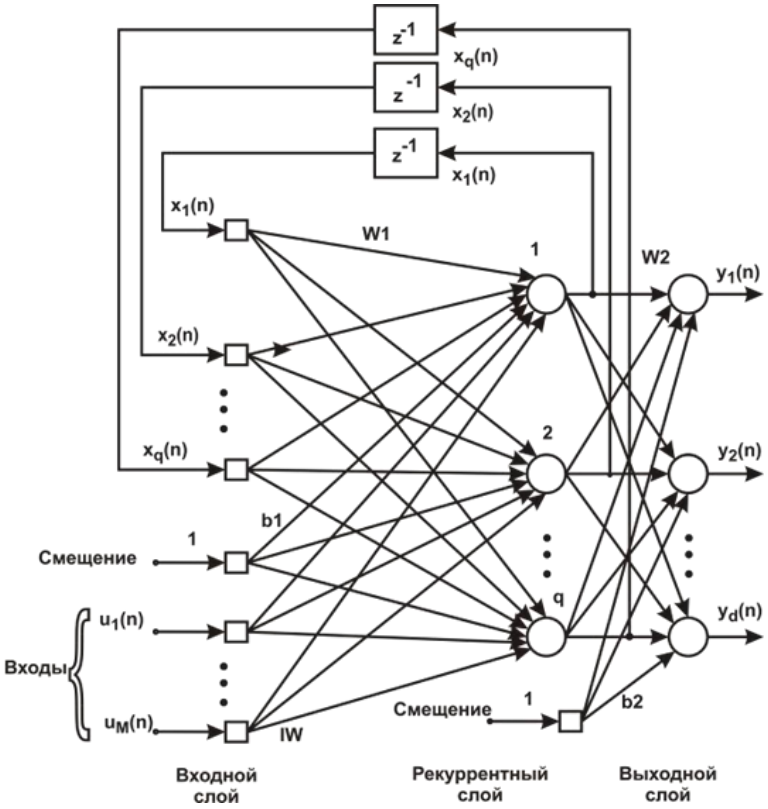

Рис. 7. Рекуррентная нейронная сеть, показаны входной, рекуррентный и выходной слои

Деревья решений представляют один из классических алгоритмов машинного обучения с учителем, решающим задачу классификации или же регрессии, представляя из себя древовидную структуру правил (предикатов).

Путем оценки входных параметров, дерево решений прогнозирует некоторое значение, которое и является результатом работы алгоритма. По виду результирующего значения различают деревья с непрерывными значениями (дерево регрессии) и деревья с некоторым заранее определенным множеством значений-метками классов (дерево классификации).

Иллюстрация классификации деревом решений приведена на рис. 8, отметим, что именно листья дерева содержат метки классов.

В задачах обнаружения вторжений часто используются наиболее распространенные модели деревьев решений, такие как, CART, C4.5 и ID3 для классификации атак. Нередко в задачах обнаружения вторжений используются ансамбли из деревьев решений, такие как Random Forest и XGBoost.

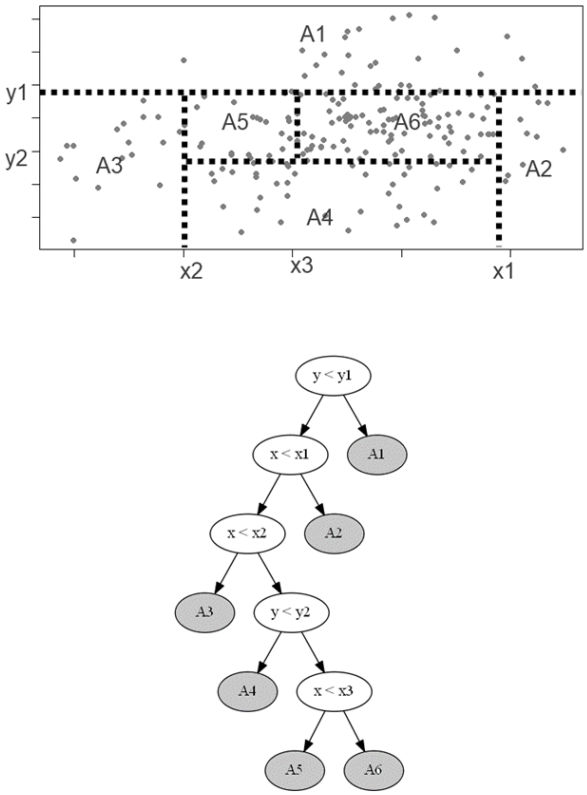

Рис. 8. Пример классфикации алгоритмом дерева решений

Метод опорных (машинных) векторов (SVM) является контролируемым алгоритмом машинного обучения, основанным разделения n-мерного пространства признаков посредством гиперплоскости разделения наибольшей ширины (рис. 9).

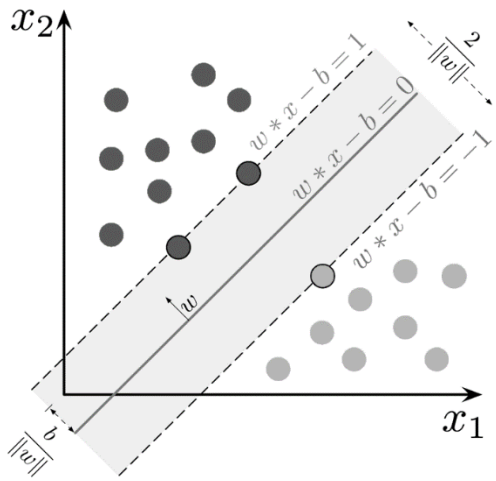

Рис. 9. Опорные вектора и оптимальная разделяющая гиперплоскость для линейно разделимого двумерного пространства

Данный метод используется для решения как линейных (когда *n*-мерное признаковое пространство возможно разбить гиперплоскостью на два непересекающихся множества), так и нелинейных задач, для нелинейных задач используются функции ядра, а такие вариации метода опорных векторов называется «ядерными SVM». Идея состоит в том, чтобы сначала отобразить входной вектор малой размерности в пространство признаков большой размерности, используя функцию ядра, причем отображение, выбирается таким образом, чтобы в новом пространстве множества были линейно разделимы, а уже затем выбирается оптимальная максимальная маргинальная гиперплоскость, которая работает как граница решения, используя функцию ядра.

В рамках обнаружения вторжений, алгоритм может быть применен для повышения точности бинарной классификации поступающих данных (разделение происходит на классы нормального и вредоносного трафика).

k ближайших соседей (*k*NN) – один из простейших алгоритмов машинного обучения с учителем, в котором используется идея «сходства признаков» для прогнозирования класса определенной выборки данных. Алгоритм идентифицирует образец на основе его соседей, вычисляя функцию расстояния до соседей (рис. 10). На рис. 10 приведен пример, когда тестовый образец (точка) будет отнесен к классу треугольников (при $k = 3$) или же к классу квадратов (при $k = 5$).

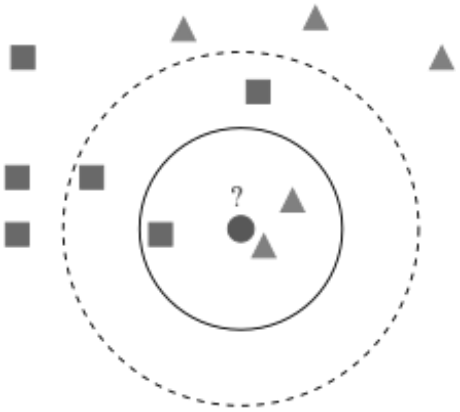

Рис. 10. Пример классификации *k*NN.

В алгоритме *k*NN параметр *k* оказывает существенное влияние на производительность модели: если значение *k* слишком мало, то модель может быть подвержена чрезмерной подгонке, а, если параметр *k* слишком велик, то может происходить неверная классификация экземпляра выборки, что было показано в работе [11].

Кластеризация представляет из себя задачу разбиения заданной выборки объектов на подмножества (кластеры), таким образом, чтобы каждый кластер состоял сравнительно схожих объектов.

Кластеризация *k*-средних – это один из популярных итеративных алгоритмов машинного обучения на основе центроидов, который обучается без учителя. Значение k является количеством центроидов (центров кластера) в наборе данных. Для назначения определенных точек данных кластеру обычно рассчитывается расстояние. Основная идея состоит в том, чтобы уменьшить сумму расстояний между точками данных и их

соответствующими центроидами внутри кластера.

Главным образом, в задаче обнаружения вторжений, данный алгоритм нашел применение для обнаружения аномалий – экземпляров атак, которые были ранее неизвестны.

Существуют и другие часто применяемые в задачах обнаружения вторжений алгоритмы кластеризации, например, DBSCAN и LOF.

Таким образом, обобщая рассмотренные методы и работы, можно указать на тенденцию к гибридизации моделей для повышения точности обнаружения вторжений, посредством, в том числе, использования методов ИАД. Кроме того, стоит отметить достаточно большой разрыв между академическими исследованиями и применением разработанных методов на практике, это может быть обусловлено сложностью сбора данных с реальных систем для последующего обучения алгоритмов. Тем не менее, представляется перспективным дальнейшие исследования в области использования методов ИАД для задач обнаружения вторжений.

Список литературы

1. DDoS-атаки в первом квартале 2022 года // SECURELIST: [сайт]. [2022]. URL: https://securelist.ru/ddos-attacks-in-q1-2022/105045/ (дата обращения: 25.06.2022).

2. Актуальные киберугрозы: I квартал 2022 года // Positive Technologies: [сайт]. [2022]. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022-q1/ (дата обращения: 12.08.2022).

3. Число DDoS-атак в России в третьем квартале выросло на 180% // ТАСС: [сайт]. [2022]. URL: https://tass.ru/ekonomika/16136633 (дата обращения: 24.10.2022).

4. Эксперты предсказали рост кибератак на российские компании в 2023 году // Swordfish Security: [сайт]. [2022]. URL: https://swordfishsecurity.ru/eksperty-predskazali-rost-kiberatak-na-rossijskie-kompanii-v-2023-godu/ (дата обращения: 01.11.2022).

5. Vinayakumar Ravi, Mamoun Alazab, Soman Kp, Prabaharan Poornachandran, A. Al-Nemrat, Sitalakshmi Venkatraman. Deep Learning Approach for Intelligent Intrusion Detection System // IEEE Access, Apr 2019.

6. Leila Mohammadpour, Teck Chaw Ling, Chee Sun Liew, Chun Yong Chong. A convolutional neural network for network intrusion detection system 2018. C. 50-55.

7. Yan B., Han G. Effective feature extraction via stacked sparse autoencoder to improve intrusion detection system // IEEE Access, T. 6, Jul 2018. C. 41238-41248.

8. Network Intrusion Detection Based on Supervised Adversarial Variational Auto-Encoder With Regularization // IEEE Access, Vol. 8, Feb 2020. pp. 42169-42184.

9. Chuanlong Yin, Yuefei Zhu, Jinlong Fei, Xinzheng He. A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks // IEEE Access, T. 5, Oct 2017. C. 21954-21961.

10. Boukhalfa A., Abdellaoui A., Hmina N., Chaoui H. LSTM deep learning method for network intrusion detection system // International Journal of Electrical and Computer Engineering, T. 10, № 3, 2020. C. 3315-3322.

11. Zhang Youqiang, Cao Guo, Wang Bisheng, Li Xuesong. A novel ensemble method for k-nearest neighbor // Pattern Recognition, T. 85, Jan 2018. C. 13-25.

МИРЭА – Российский технологический университет
MIREA – Russian Technological University

Поступила в редакцию 5.11.2022

Информация об авторах

Лось Владимир Павлович – д-р воен. наук, профессор, МИРЭА - Российский технологический университет, e-mail: mnac@comch.ru

Маланьин Данила Дмитриевич – аспирант, МИРЭА - Российский технологический университет, e-mail: mnac@comch.ru

METHODS OF INTELLIGENT DATA ANALYSIS USED IN THE INTRUSION DETECTION

V.P. Los, D.D. Malanin

The development of information technology has caused a dramatic increase in the number of attacks on information system components, which, in turn, has made the task of intrusion detection more relevant and important than ever. The use of data mining methods provides ample opportunities in various fields of science and technology, including for solving information security problems. This article proposes a classification of intrusion detection systems according to various criteria. A review of popular methods of data mining, which are widely used in other fields of science, is given in the context of application to the problem of intrusion detection. An approach to solving intrusion detection problems using a recurrent neural network is considered.

Keywords: information security, intrusion detection system, data mining methods.

Submitted 5.11.2022

Information about the authors

Vladimir P. Los – Dr. Sc. (Military), Professor, MIREA - Russian Technological University, e-mail: mnac@comch.ru

Danila D. Malanin – Graduate Student, MIREA - Russian Technological University, e-mail: mnac@comch.ru