DOI 10.36622/VSTU.2023.26.3.024
УДК 004.056

НЕЙРОСЕТЕВАЯ МОДЕЛЬ ДЛЯ ПОВЫШЕНИЯ ТОЧНОСТИ ОБНАРУЖЕНИЯ СЕТЕВЫХ ВТОРЖЕНИЙ

С.А. Ермаков, А.Г. Чурсин, П.А. Анцупов

Разработана модель обнаружения сетевых вторжений, с использованием нейросетевых структур, главным отличием которой является более точная идентификация угроз, по сравнению с аналогами. Проанализированы публикации по темам выявления угроз информационной безопасности, особенностям применения машинного обучения и эффективности использования моделей нейронных сетей с глубоким обучением для обнаружения атак. Выделены нерешенные частные проблемы, требующие детальной проработки: выбор наиболее оптимальной архитектуры нейронной сети, и комбинирование методов статистического анализа и машинного обучения. Представлена модель системы обнаружения вторжений и вредоносной активности, которая сочетает в себе аналитику поведения пользователей и модель выявления аномалий. Предложенная модель позволяет отслеживать кибератаки, для которых отсутствуют сигнатуры, и снизить уровень ложных срабатываний при идентификации ранее неизвестных кибератак.

Ключевые слова: атака, информационная система, нейронная сеть, пользователь.

Введение

С прогрессом цифровых технологий происходит и развитие киберпреступности, которая использует в своих противозаконных действиях уязвимости информационных систем. Широкий спектр новых и развивающихся угроз в киберпространстве вынуждает отрасль информационной безопасности находиться в состоянии постоянной готовности. Вредоносные программы, фишинг, изощренные кибератаки с использованием искусственного интеллекта и машинного обучения подвергают информацию и активы компаний, государственных органов и частных лиц постоянному риску.

Немаловажным фактором, который способствует росту атак в информационных сетях является стремительное увеличение объема информации в электронном виде. Согласно компании Statista до 2025 года, объем создаваемых глобальных данных вырастет до более чем 180 зеттабайт (рис. 1).

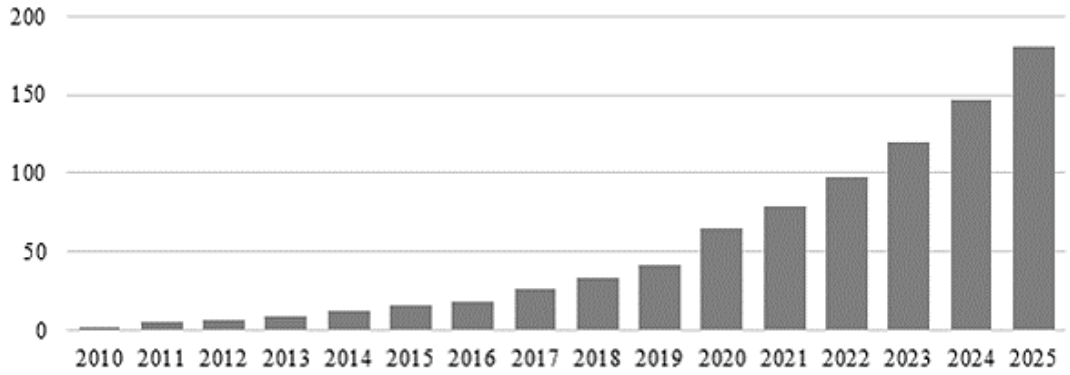

Рис. 1. Объем данных в электронном виде во всем мире (в зеттабайтах) [1]

На сегодняшний день существует множество разнообразных методов и средств защиты от кибератак в различных информационных системах. Однако, следует отметить то, что до сих пор не выработано абсолютно универсального метода противодействия атакам и поэтому возникает необходимость комплексного подхода к решению данной задачи.

Традиционные методы обнаружения вторжений, которые автоматизируют процесс контроля событий, происходящих в информационной системе, не дают ожидаемого результата. Это в свою очередь определяет необходимость использования более эффективных методов обнаружения, в том числе тех, которые основаны на искусственном интеллекте.

Применение методов интеллектуального анализа данных и искусственного интеллекта позволяет повысить эффективность противодействия вторжениям и защитить объекты от потенциальных нарушителей. Ряд современных систем обнаружения вторжений используют разные методы интеллектуального анализа данных для выявления атак. В основе таких систем лежат разные методики: методы Data Mining; поиск ассоциативных правил; марковские процессы; деревья принятия решений; генетические алгоритмы; нейронные сети [2].

Таким образом, рассмотрение возможностей нейронных сетей для выявления закономерностей в поведении информационных систем, определения аномального поведения и противодействия компьютерным атакам, является на сегодняшний день актуальным направлением исследования.

Анализ публикаций по теме исследования.

Описание примеров и способов применения нейросетевых технологий для выявления угроз информационной безопасности представлено в ряде научных работ зарубежных и отечественных авторов, из числа которых можно выделить Алексеенко С.П., Достова В.В., Баева Н.А., Бурнашева Р.У. Lin, Si-Chen; Huang, Szu-Chun; Lei, Chin-Laung; Huang, Chun-Ying.

Особенности применения методов машинного обучения (дерево решений (DT), линейной регрессии (LR), случайного леса (RF) и машины опорных векторов (SVM)) для обнаружения вторжений в различные информационные сети рассматривались Покровской Н.Н., Букиным А.В., Самоновым А.В., Тихоновым Э.И., Zhang, Zeping; Wang, Xiaowen; Zhang, Shuaishuai; Huang, Jie.

Эффективность использования моделей нейронных сетей с глубоким обучением для обнаружения различных атак, а именно ботнета, DoS, проникновения нашла свое отражение в публикациях Касеновой А.У., Кульмамирова С.А., Микрюкова А.А., Бабаша А.В., Сизова В.А., Srivastava, Gautam; Fouda, Mostafa M.

Нерешенные части общей проблемы

Несмотря на широкий интерес к рассматриваемой проблематике, ряд вопросов в данной предметной плоскости требует углубленного исследования. В частности, особого внимания заслуживает проблема выбора наиболее оптимальной архитектуры нейронной сети с относительно небольшим количеством параметров, поскольку меньшее количество параметров приведет к меньшей задержке при обнаружении онлайн-атак. Также в более детальной проработке нуждаются возможности комбинирования статистического анализа и машинного обучения для повышения эффективности алгоритмов обнаружения кибератак.

Цель работы

Заключается в повышении точности обнаружения вторжений и вредоносной активности. Задачей исследования является разработка модели обнаружения сетевых вторжений на основе нейросетевых структур.

Результаты

Современные методы выявления программно-технических воздействий, приводящие к инцидентам информационной безопасности, можно разделить на две основные категории: распознавание поведения пользователя и выявление аномалий. Методы распознавания злоупотреблений, которые описываются с помощью сигнатур известных кибератак, обладают высокой точностью и низким уровнем ошибочных срабатываний, но не способны обнаруживать кибератаки, для которых отсутствуют сигнатуры [3]. Методы выявления аномалий позволяют идентифицировать ранее неизвестные кибератаки, но обладают высоким уровнем ложных срабатываний [4].

Нейронные сети являются альтернативой компонентам статистического анализа систем обнаружения атак. Нейросети позволяют отследить типовые характеристики сетевого трафика и идентифицировать статистически значимые отклонения от установленного режима работы. Они получили широкое распространение из-за их способности к самообучению. Более того, нейросеть можно настроить так, чтобы она и дальше самостоятельно совершенствовалась, постоянно реагируя на малейшие изменения в локальной сети [5].

Таким образом, на рис. 2 изображена разработанная модель системы обнаружения атак в информационных сетях с использованием нейроструктур.

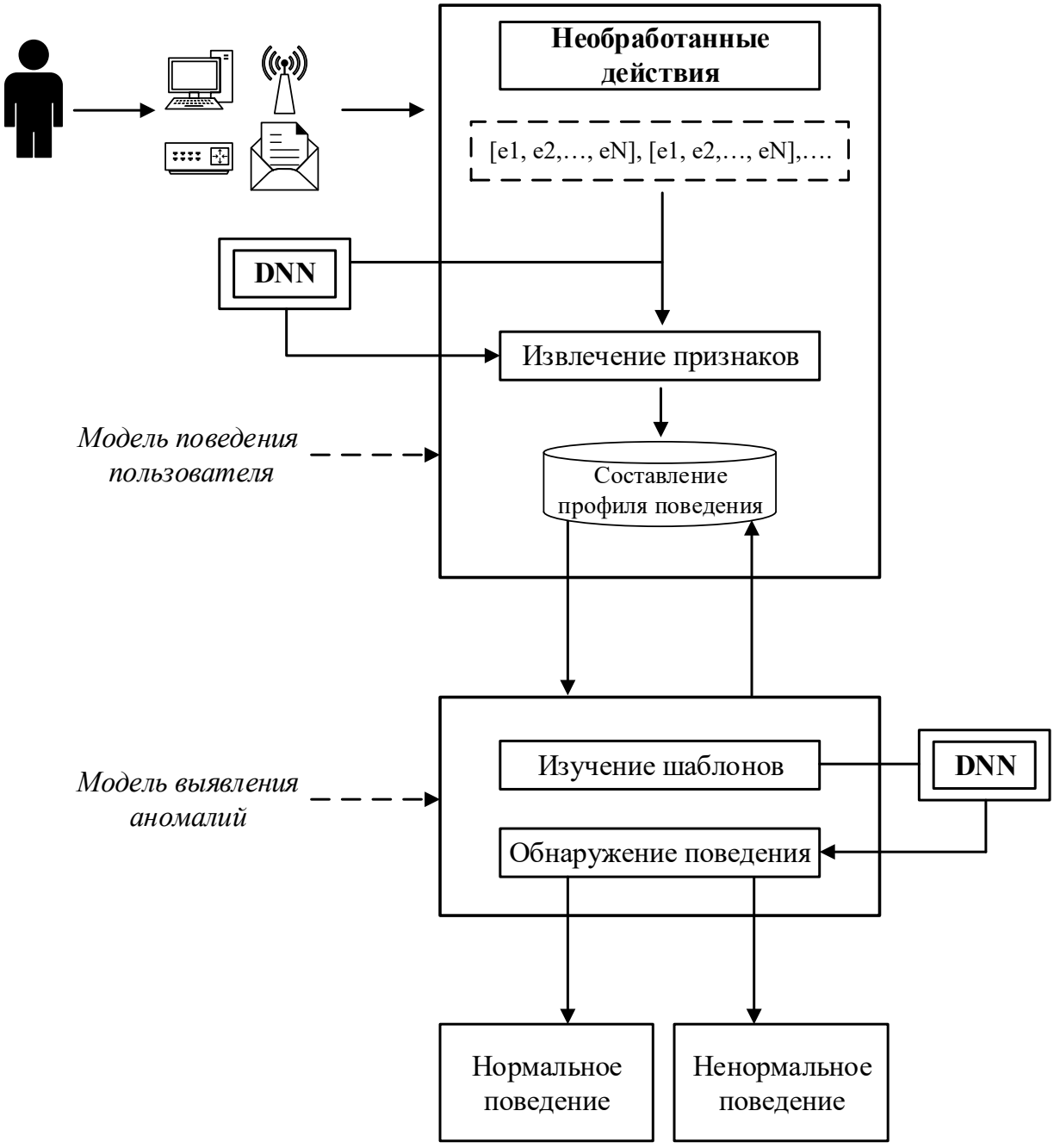

Рис. 2. Модель системы обнаружения атак в информационных сетях с использованием нейронной сети

Модель системы обнаружения атак предполагает использование искусственной нейронной сети, а именно глубокой нейронной сети и для распознавания поведения пользователей, и для выявления аномалий.

Глубокая нейронная сеть является частью искусственного интеллекта и относится к семейству контролируемых методов обучения модели с помощью нескольких слоев [6]. Структура DNN включает входной слой, несколько скрытых слоев и выходной слой.

Пусть $X = \{x_1, x_2, ..., x_n\}$ - входной вектор с n признаками, а $Y = \{y_1, y_2, ..., y_n\}$ - выходной вектор, состоящий из значений вероятности в диапазоне [0,1]. Значения вероятности складываются в 1 для классификации нормальных (отсутствие атаки) и аномальных (ARP Spoofing, DoS-атака, Nmap PortScan и Smurf-атака) атак. Оценка выхода каждого скрытого слоя (HL) приведена в уравнении:

$$HL_i = A(wi + bi), \tag{1}$$

где A - обозначает нелинейную функцию активации, w_i и b_i - вес и смещение скрытого слоя (i). В скрытом и выходном слоях применяются функции активации «ReLU» и «Softmax» соответственно. Функция активации ReLU реализуется с помощью уравнения:

$$\mathrm{Re}\,LU(x) = \max(0, x), \tag{2}$$

Softmax содержит вектор в диапазоне [0,1], который применяется к результативным оценкам (rs). Каждый элемент обозначает класс и имеет возможность определять вероятности классов. Функция Softmax используется для всех элементов (rs). Для любого заданного класса rs_i функция Softmax вычисляется в соответствии со следующим выражением:

$$f(rs_i) = \exp rs_i / \sum_j^c \exp rs_j, \tag{3}$$

где rs_j - оценки результатов, полученные сетью для каждого класса в C.

Функция активации Softmax для класса rs_i опирается на все оценки в rs. Структура DNN, используемая в предлагаемой модели, состоит из входного слоя с пятью нейронами, обозначающими набор признаков; двух плотных слоев с восемью нейронами и слоя классификации Softmax, состоящего из пяти выходов для обозначения нормальных и аномальных атак.

Разработанная модель работает следующим образом:

На первом шаге модель профилирует поведение пользователей. Задача состоит в том, чтобы собрать различные события данных разных типов, связанные с деятельностью пользователя. Профилирование поведения пользователя позволяет найти такие шаблоны, которые будут означать подозрительное поведение независимо от того, исходят ли эти события от киберпреступника, инсайдера или вредоносного ПО. Анализ поведения пользователя не предотвращает атаку, а помогает выявить и оценить потенциальную возможность атаки через действия пользователя. Данные о поведении пользователя могут быть получены как из текущих, так и из прошлых его действий. Собранные данные могут включать в себя различные значения, например, идентификатор пользователя и его IP-адрес.

Полученные данные структурируются как серия событий, в которой каждое событие состоит из одного или нескольких данных. Задача состоит в том, чтобы на основе автоматического извлечения признаков построить отличительный профиль пользователя.

Характеристики извлекаются из последовательности действий каждого

пользователя. Каждая последовательность индексируется по времени, в которое она была получена. Если задана последовательность действий пользователя *S*, то она представляется в виде потока событий, таких что:

$$S = \{e_1, e_2, ..., e_n\}, \tag{4}$$

где $n \in N$ длина потока. Для события e_i - это набор точек данных, таких, что:

$$e_i = \{p_1, p_2, ..., p_i\}, \tag{5}$$

где $p_j \in R$ - обозначает вектор входных серий.

Таким образом, признак может быть извлечен из потока данных для работы с абстрактными формами признаков.

Перед извлечением признаков важно провести нормализацию данных для более эффективного их использования нейронной сетью. Причина заключается в том, что выходы функции активации достигают точки насыщения, после которой они остаются постоянными [7]. Поэтому при использовании ячеек DNN необходимо обеспечить правильную нормализацию входов, чтобы выходы не попадали в область насыщения. Таким образом, следующим шагом является нормализация экземпляров числовых данных к диапазону от 0 до 1. Для этого предлагаем использовать общепринятую формулу нормализации min-max scaling.

Таким образом, вектор p_j, который представляет собой серию входящих определенных точек данных, масштабируется по $p \in [0,1]$ как показано в уравнении (6):

$$p = \frac{p_{j-\min}(p_j)}{\max(p_j) - \min(p_j)}, \tag{6}$$

Последовательность действий передается в DNN в виде вектора для извлечения признаков из исходных данных, таким образом, идея заключается в построении абстрактного пространства признаков. DNN является универсальным аппроксиматором и имеет преимущество, которое заключается в том, что петли обратной связи ячеек с самого начала учитывают временной порядок, а также временные зависимости последовательностей [8]. Для оптимального извлечения признаков из последовательной структуры полученных данных целесообразным является использовать длинную кратковременную память (LSTM) для отображения идеального пространства признаков. Таким образом, LSTM применяется для получения абстрагированного вектора признаков с помощью глубокого слоя из исходных данных, что в итоге позволяет определить, является ли это поведение нормальным или вредоносным.

На втором шаге модель обнаруживает атаки в информационных сетях путем выявления аномалий.

Предлагаемая система состоит из двух этапов обнаружения различных типов кибератак, таких как ARP Spoofing, DoS-атаки, Nmap-атаки и Smurf-атаки (рис.3). Этими двумя этапами являются

1) этап подготовки данных;

2) этап обнаружения атак на основе DNN.

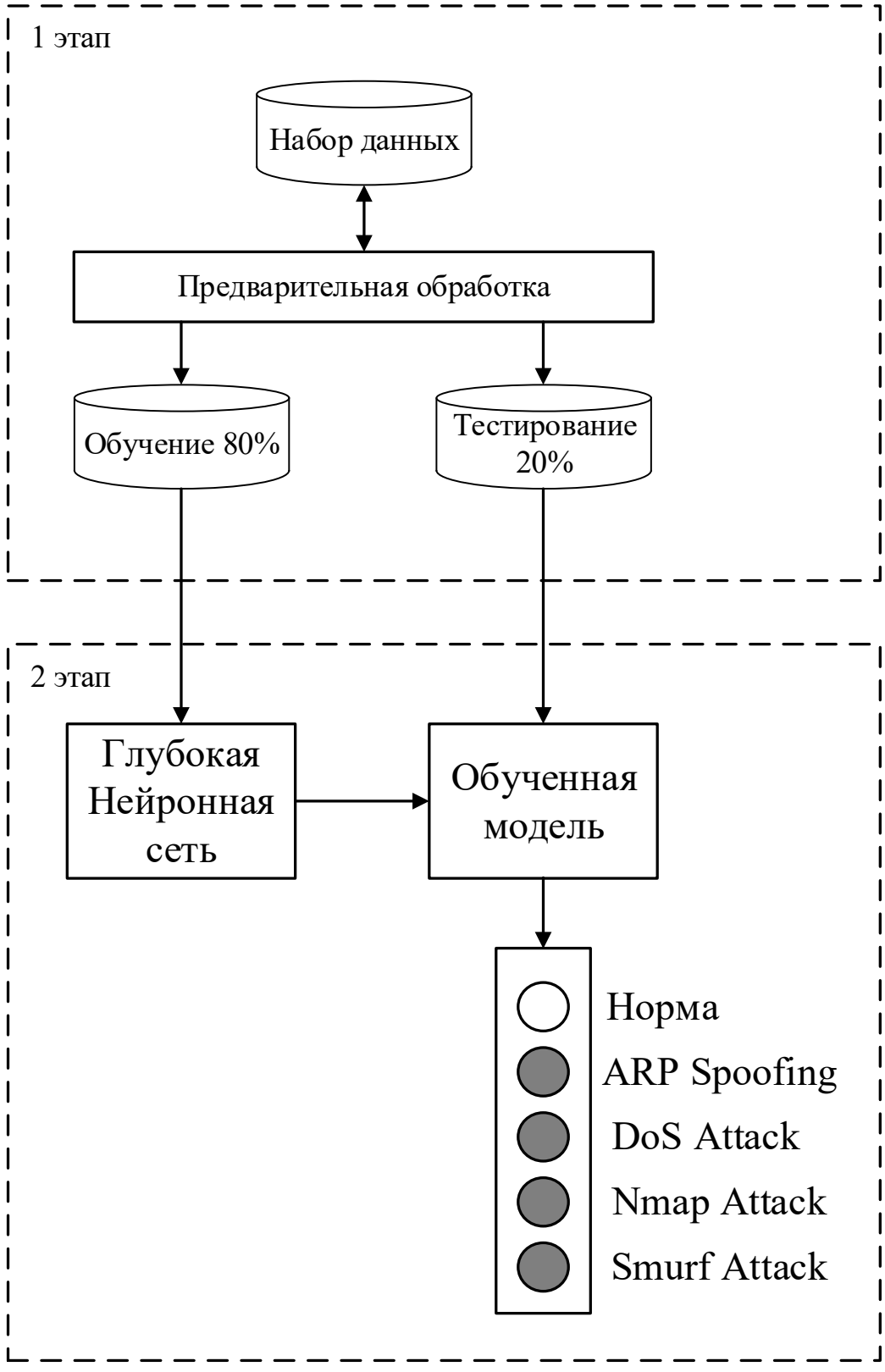

Рис. 3. Алгоритм работы модели выявления аномалий

Модель DNN работает следующим образом:

1) для анализа различных кибератак используется набор данных;

2) из этого набора данных извлекаются пять признаков, а для кодирования категориальных признаков используется одноточечное кодирование;

3) для подготовки к многоклассовой классификации набор данных маркируется

как нормальный, ARP Spoofing, DoS-атака, Nmap-атака и Smurf-атака;

4) набор данных разделяется на обучающий и тестовый наборы, составляющие 80% и 20% соответственно;

5) DNN учится на выбранном наборе данных, выбирая метки в качестве целевых признаков с помощью многоклассовой классификации, и создает обучаемую модель;

6) обученная модель DNN тестируется на тестовом наборе данных для предсказания нормальных или других типов атак.

Таким образом объединение модели поведения пользователя и модели обнаружения аномалий позволяет более точно идентифицировать угрозы.

Заключение

Проанализированы работы по темам выявления угроз информационной безопасности, особенностям применения машинного обучения и эффективности использования моделей нейронных сетей с глубоким обучением для обнаружения атак. Выделены нерешенные частные проблемы, требующие детальной проработки: выбор оптимальной архитектуры нейронной сети и комбинирование методов статистического анализа и машинного обучения. Разработана модель системы обнаружения атак в информационных сетях с использованием нейронной сети, которая сочетает в себе аналитику поведения пользователей и модель выявления аномалий. Благодаря объединению этих двух блоков обеспечивается более точная идентификация угроз по сравнению с другими подходами, поскольку глубокое обучение обладает повышенной способностью к самообучению и адаптации, обобщению и обнаружению неизвестной атаки.

Список литературы

1. Volume of data/information created, captured, copied, and consumed worldwide. Statista. URL: https://www.statista.com/statistics/871513/worldwide-data-created/

2. Курбанов А.И. Методы для обнаружения атак в информационных сетях // Endless Light in Science. 2022. № 7-7. С. 101-105.

3. Лихтциндер Б.Я. Информационная безопасность беспроводных сенсорных сетей (угрозы и защита) // Вестник связи. 2021. № 2. С. 8-17.

4. Li, Ju Research on an optimised encryption algorithm for network information security communication // International journal of communication networks and distributed systems. 2023. Volume 29: Number 1; pp 31-46.

5. Язов Ю.К. Применение составных сетей петри-маркова при математическом моделировании угроз безопасности информации // Охрана, безопасность, связь. 2023. № 8-2. С. 185-196.

6. Фисун В.В. Методика оценки защищенности в интеллектуальной системе управления информационной безопасностью объектов критической информационной инфраструктуры // Национальная Ассоциация Ученых. 2022. № 77. С. 59-62.

7. Ma, Yajing Neural network-based secure event-triggered control of uncertain industrial cyber-physical systems against deception attacks // Information sciences. 2023. Volume 633; pp 504-516.

8. Zhang, Yuhan Neural-Network-Based Secure State Estimation Under Energy-Constrained Denial-of-Service Attacks: An Encoding-Decoding Scheme // IEEE transactions on network science and engineering. 2023. No 4; pp 2002-2015.

Концерн «Созвездие»
Concern Sozvezdie

Воронежский государственный технический университет
Voronezh State Technical University

Поступила в редакцию 9.09.2023

Информация об авторах

Ермаков Сергей Александрович – канд. техн. наук, начальник отдела, Концерн «Созвездие», доцент, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

Чурсин Андрей Германович – аспирант, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

Анцупов Павел Андреевич – аспирант, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

NEURAL NETWORK MODEL FOR IMPROVING THE ACCURACY OF NETWORK INTRUSION DETECTION

S.A. Ermakov, A. G. Chursin, P.A. Antsupov

A model for detecting network intrusions using neural network structures has been developed, the main difference of which is a more accurate identification of threats compared to analogues. Analyzed publications on the topics of identifying information security threats, the specifics of using machine learning and the effectiveness of using neural network models with deep learning to detect attacks. The unsolved parts requiring detailed study are highlighted: the choice of the most optimal neural network architecture, and the combination of statistical analysis and machine learning methods. A model of an intrusion detection system and malicious activity is presented, which combines user behavior analytics and an anomaly detection model. The proposed model allows you to track cyber-attacks for which there are no signatures and reduce the level of false positives when identifying previously unknown cyber-attacks.

Keywords: attack, information system, neural network, user.

Submitted 9.09.2023

Information about the authors

Sergey A. Ermakov – Cand. Sc (Technical), Head of Department, Concern Sozvezdie, Associated Professor, Voronezh State Technical University, email: alexanderostapenkoias@gmail.com

Andrey G. Chursin – Graduate Student, Voronezh State Technical University, email: alexanderostapenkoias@gmail.com

Pavel A. Antsupov – Graduate Student, Voronezh State Technical University, email: alexanderostapenkoias@gmail.com