ТЕХНИЧЕСКИЕ НАУКИ

УДК 004.042

Обзор нейросетевых технологий в системах обнаружения вторжений в сети

Т.А. Исакова
Донской государственный технический университет, г. Ростов-на-Дону, Российская Федерация

Аннотация
Рассматривается проблема выявления сетевых атак на информационный поток. Эффективное и оперативное обнаружение потенциальных сетевых угроз является ключевым фактором для обеспечения безопасности информационного потока от несанкционированного доступа. Описаны различные подходы к обнаружению сетевых атак, проводится анализ методов, основанных на применении нейронных сетей, а также осуществляется обзор приложений, предназначенных для анализа сетевого трафика и выявления случаев несанкционированного доступа к информационному потоку.

Ключевые слова: сетевые атаки, несанкционированный доступ, информационный поток, информационная безопасность, базы данных, обнаружение атак, нейронные сети, защита информации

Для цитирования. Исакова Т.А. Обзор нейросетевых технологий в системах обнаружения вторжений в сети. *Молодой исследователь Дона.* 2025;10(3):14–16.

Overview of Neural Network-Based Technologies Used in the Network Intrusion Detection Systems

Tatyana A. Isakova
Don State Technical University, Rostov-on-Don, Russian Federation

Abstract
The article studies the problem of detecting the network attacks on the information flow. Efficient and prompt detection of the potential network threats is crucial for ensuring the information flow security and preventing it from unauthorized access. Various approaches to network attack detection have been described, and the neural network-based technologies have been analysed. The applications for network traffic analysis and detection of unauthorized access to information flow have been overviewed.

Keywords: network attacks, unauthorized access, information flow, information security, databases, detection of the attacks, neural networks, information protection

For Citation. Isakova TA. Overview of Neural Network-Based Technologies Used in the Network Intrusion Detection Systems. *Young Researcher of Don.* 2025;10(3):14–16.

Введение. Важной задачей в области защиты информации является процесс обнаружения сетевых атак на базы данных. Успешная атака на информационный поток свидетельствует о том, что злоумышленники получили несанкционированный доступ к данным. В данной статье мы рассмотрим проблему обнаружения сетевых атак на информационный поток. Эта проблема становится особенно актуальной в современных реалиях, поскольку почти все отрасли деятельности перешли на систему электронного документооборота, что указывает на существенное увеличение объема информации, передаваемой по сети. Цель статьи заключается в анализе подходов к обнаружению сетевых атак, исследовании методов, использующих нейронные сети, и обзоре приложений для анализа сетевого трафика и выявления несанкционированного доступа к информационному потоку.

Описание проблемы. Постоянное увеличение объемов информации, передаваемой по сети, создает необходимость в модернизации методов защиты данных. Проблема обеспечения безопасности информации имеет как организационный, так и технологический аспекты. Организационный аспект включает в себя реализацию систем обнаружения сетевых атак и принятие мер по дополнительному копированию наиболее важной информации на внешние носители. Технологический аспект касается установления ограничений на использование подозрительных ссылок и обновлений в информационной системе.

Основная часть. Атака на сеть представляет собой несанкционированный доступ к сети и к информации, передаваемой по ней, с использованием технических средств и программного обеспечения. Сетевые атаки классифицируются по нескольким критериям:

1. По характеру воздействия: активные атаки (нарушают нормальную работу системы) и пассивные атаки (влияют на политику безопасности, не оказывая прямых воздействий на функционирование системы).

2. По цели: атаки, направленные на нарушение нормальной работоспособности системы, и атаки, нарушающие доступ к системе.

3. По наличию связи с программным средством злоумышленника: атакующие могут иметь доступ к информации о реакции сети на атаку (при наличии связи) или не иметь такой возможности (при отсутствии связи).

4. По местоположению злоумышленника: межсегментные атаки (злоумышленник находится вдали от атакуемой системы) и внутрисегментные атаки (злоумышленник находится вблизи атакуемой системы).

Оперативное обнаружение возможных сетевых атак способствует защите информационного потока от несанкционированного доступа. Эффективность процесса своевременного реагирования на подозрительный доступ к сети во многом зависит от используемого метода. В научной статье «Исследование методов обнаружения сетевых атак» автор Гаврилова Е.А. подробно освещает методы обнаружения сетевых атак, включая статистический анализ, экспертные системы и нейронные сети. Далее мы проанализируем указанные методы и выделим их особенности.

Статистический анализ предполагает мониторинг точной последовательности действий при использовании сети: любое отклонение от установленного сценария будет интерпретироваться как несанкционированный доступ. Однако можно адаптировать систему защиты в ответ на действия пользователей, добавляя в сценарий варианты, которые будут считаться безопасными. Экспертные системы также применяются для защиты данных от несанкционированного доступа. Их работа основывается на заранее заданных шаблонах, описывающих процесс атаки. Если система обнаруживает действия, аналогичные тем, что перечислены в шаблонах, они классифицируются как угрозы. Данный метод защиты не допускает ложных срабатываний, однако требует постоянного обновления информации об атаках, что осуществляется вручную, без возможности использования автоматизации.

Третий метод, рассмотренный автором статьи, включает в себя применение нейронных сетей для защиты данных. Этот подход является более эффективным благодаря способности обрабатывать значительные объемы информации и работать с большим объемом сетевого трафика, который может изменяться по активности [1]. К преимуществам использования нейронных сетей в защите баз данных и сетевой инфраструктуры от атак можно отнести следующие аспекты:

1. Адаптация к любым видам информации;

2. Быстрый анализ сетевого потока и оперативное выявление несанкционированного доступа;

3. Прогнозирование действий злоумышленников в сети;

4. Анализ характеристик атак на информационный поток.

Нейронные сети представляют собой модели с программными функциями, которые имитируют структуру человеческих нейронов, заменяя их машинными аналогами. Иными словами, это системы с искусственным интеллектом, предназначенные для выполнения задач, ранее отводимых человеку. К функционалу нейросетей относятся задачи, связанные с:

1. Распознаванием образов: на вход сети подаются изображения или описания объектов;

2. Кластеризацией: распознавание характеристик образов и их классификация по категориям на основе сходств;

3. Аппроксимацией: оценка неизвестных функций по известным значениям;

4. Оптимизацией: нахождение решений, удовлетворяющих заданным условиям.

Сетевые атаки делятся на четыре вида:

1. DoS (Denial of Service);

2. U2R (User to Root);

3. R2L (Remote to Local);

4. Probe (расследование).

DoS-атаки направлены на создание отказа в работе системы за счет чрезмерного сетевого трафика, который перегружает и блокирует сервер. U2R-атаки стремятся получить злоумышленниками статус администратора сети. R2L-атаки нацелены на доступ к серверу незарегистрированным пользователем через несанкционированный компьютер. Probe-атаки осуществляются для сканирования сетевых портов с целью кражи информации, передаваемой по сети [5].

В научной статье «Разработка приложения для анализа сетевого трафика и обнаружения сетевых атак» авторов Иванова А.Д., Кутищева А.А. и Никитина Е.Ю. рассматривается разработка программного обеспечения для выявления несанкционированного доступа к данным в сети с использованием нейронных сетей. Авторы акцентируют внимание на том, что система защиты должна уметь распознавать как известные, так и ранее не встречавшиеся виды атак. С помощью нейронной сети система отслеживает подозрительную активность в сетевом трафике и без вмешательства оператора фиксирует случаи несанкционированного доступа. Идея рассмотренного приложения заключается в его способности самостоятельно, без вспомогательного оборудования, собирать полную информацию о сетевых подключениях. Затем информация о сетевом трафике проходит обработку и классификацию.

Работа над системой обнаружения сетевых атак началась с проектирования нейросетевого модуля, для чего был использован набор данных о сетевых вторжениях CSE-CIC-IDS2018. В качестве инструмента для обучения нейросети была выбрана библиотека PyTorch для языка программирования Python [2]. Данный набор данных содержит информацию о безопасных соединениях и классах сетевых атак. Подбор количества нейронов на скрытых слоях был реализован с помощью вычислений, основанных на формуле, где число нейронов в скрытом слое равно квадратному корню произведения числа нейронов во входном и выходном слоях. Для повышения точности работы нейронных сетей применялась оптимизация входных параметров, в результате чего был получен набор из 30 параметров о соединениях в сети.

В систему обнаружения сетевых атак также входит сетевой анализатор, который обеспечивает получение информации обо всем трафике. Авторы использовали CICFlow-meter-V4.0, написанный на языке программирования Java [3]. Этот инструмент не только предоставляет данные о трафике, но и передает их в базу данных. База данных или хранилище информации нужны для обработки и хранения полученных данных, которые затем должны быть проанализированы на предмет наличия сетевых атак [4].

В ходе разработки системы обнаружения сетевых атак была создана нейросетевая модель однослойного персептрона с 88 нейронами, обладающая высокой точностью и эффективностью в реализации своих функций.

Заключение. Таким образом, система обнаружения несанкционированного доступа к информационному потоку является необходимой мерой защиты от атак на базы данных. В настоящее время данная система представляет собой программное обеспечение, автоматизирующее процессы и обеспечивающее эффективный контроль за возможными вторжениями в сеть. В данной статье были рассмотрены подходы к обнаружению сетевых атак, проанализированы методы с использованием нейронных сетей и проведен обзор приложений для анализа сетевого трафика и выявления несанкционированного доступа к информационному потоку. Перспективы развития систем обнаружения атак могут включать внедрение функций автоматического распознавания новых видов атак, а также адаптацию и улучшение методов борьбы с ними.

Список литературы

1. Гаврилова Е.А. Исследование методов обнаружения сетевых атак. *Научные записки молодых исследователей.* 2017;12(2):55–58.

2. *CSE-CIC-IDS2018 on AWS. Canadian Institute for Cybersecurity*. URL: https://www.unb.ca/cic/datasets/ids-2018.htm (accessed: 10.02.2025).

3. Ясницкий Л.Н. *Интеллектуальные информационные технологии и системы*. Учебно-методическое пособие. Пермь: Пермский государственный университет; 2007. 271 с.

4. Иванов А.Д., Кутищев А.А., Никитина Е.Ю. Разработка приложения для анализа сетевого трафика и обнаружения сетевых атак. *Вестник Пермского университета Серия: Математика. Механика. Информатика.* 2021;2(53):57–64.

5. Боршевников А.Е. Сетевые атаки. Виды. Способы борьбы. В: *Труды Международной научной конференции «Современные тенденции технических наук». Уфа, октябрь 2011 года*. Уфа: Лето; 2011. С. 8.

Об авторах:

Татьяна Александровна Исакова, студент кафедры кибербезопасности информационных систем Донского государственного технического университета (344003, Российская Федерация, г. Ростов-на-Дону, пл. Гагарина, 1), isakovatttt@yandex.ru

Конфликт интересов: **авторы заявляют об отсутствии конфликта интересов.**

Все авторы прочитали и одобрили окончательный вариант рукописи.

About the Author:

Tatyana A. Isakova, Student of the Cybersecurity of Information Systems Department, Don State Technical University (1, Gagarin Sq., Rostov-on-Don, 344003, Russian Federation), isakovatttt@yandex.ru

Conflict of Interest Statement: **the author declares no conflict of interest.**

The author has read and approved the final manuscript.