Автоматизация и моделирование в проектировании и управлении. 2025. № 4 (30). С. 24-32.
ISSN 2658-3488 print, ISSN 2658-6436 online
Automation and modeling in design and management. 2025. № 4 (30). P. 24-32.

Математическое и компьютерное моделирование

Научная статья
Статья в открытом доступе
УДК 004.94
doi: 10.30987/2658-6436-2025-4-24-32

АВТОМАТИЗАЦИЯ МОДЕЛИРОВАНИЯ СИСТЕМЫ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ С ИСПОЛЬЗОВАНИЕМ НЕЙРОСЕТЕЙ

Людмила Борисовна Филиппова[1]✉, Юрий Алексеевич Леонов[2], Алексей Александрович Мартыненко [3], Родион Алексеевич Филиппов[4], Марина Георгиевна Гринь[5]
[1, 2, 3, 4, 5] Брянский государственный технический университет, г. Брянск, Россия
[1] libv88@mail.ru, https://orcid.org/0000-0002-1894-2739
[2] yorleon@yandex.ru, https://orcid.org/0000-0002-7027-7481
[3] martynenko_alex@mail.ru, https://orcid.org/0000-0002-7598-3895
[4] redfil@mail.ru, https://orcid.org/0000-0002-1365-4332
[5] marinagrin-3@mail.ru, https://orcid.org/0000-0003-2070-6281

Аннотация. *Статья посвящена актуальной проблеме анализа сетевого трафика и интеграции систем безопасности организации с использованием нейросетей. Приведена статистика видов киберугроз и сделан вывод об усложнении различных видов кибератак. Рассмотрены современные подходы к выявлению аномалий в трафике, предотвращению кибератак и анализу данных систем видеонаблюдения. Особое внимание уделено проектированию информационно-аналитической системы, способной не только детектировать угрозы в сетевом трафике, но и анализировать изображения с камер видеонаблюдения для выявления потенциальных нарушителей. Было проведено сравнительное исследование различных моделей нейронных сетей. На основании проведенного анализа был сделан вывод о повышении точности обрабатываемых данных в виде сетевого трафика и видеопотока данных. После проведенных исследований в качестве основной модели для обучения были приняты рекуррентные сети. Затем был рассмотрен анализ рекуррентных нейронных сетей (RNN) для обработки временных зависимостей в сетевом трафике и сверточных нейронных сетей (CNN) для анализа лиц из базы данных организации. Представлены результаты тестирования системы, осуществлено компьютерное моделирование, проведена оценка её эффективности в обнаружении сетевых угроз и идентификации подозрительных объектов по видеоданным.*

Ключевые слова: анализ сетевого трафика, киберугрозы, машинное обучение, сверточные нейронные сети, рекуррентные нейронные сети, видеонаблюдение, идентификация лиц, информационная безопасность

Для цитирования: Филиппова Л.Б., Леонов Ю.А., Мартыненко А.А., Филиппов Р.А., Гринь М.Г. Автоматизация моделирования системы безопасности организации с использованием нейросетей // Автоматизация и моделирование в проектировании и управлении. 2025. №4 (30). С. 24-32. doi: 10.30987/2658-6436-2025-4-24-32.

Original article
Open Access Article

AUTOMATING SAFETY SYSTEM MODELLING IN ORGANIZATIONS USING NEURAL NETWORKS

Lyudmila B. Filippova[1]✉, Yuri A. Leonov[2], Alexey A. Martynenko[3], Rodion A. Filippov[4], Marina G. Grin[5]
[1, 2, 3, 4, 5] Bryansk State Technical University, Bryansk, Russia
[1] libv88@mail.ru, https://orcid.org/0000-0002-1894-2739
[2] yorleon@yandex.ru, https://orcid.org/0000-0002-7027-7481
[3] martynenko_alex@mail.ru, https://orcid.org/0000-0002-7598-3895
[4] redfil@mail.ru, https://orcid.org/0000-0002-1365-4332
[5] marinagrin-3@mail.ru, https://orcid.org/0000-0003-2070-6281

Abstract. *The article addresses the pressing issue of network traffic analysis and integration of organizational security systems using neural networks. It provides statistics on types of cyber threats and concludes that various kinds of cyberattacks are becoming increasingly complex. The authors review modern approaches to detecting anomalies in traffic, preventing cyberattacks, and analysing surveillance camera data; give special attention to designing an information-analytical system capable of identifying threats in network traffic and analysing video footage to detect potential offenders. The authors conduct a comparative study of different neural network models, which concludes that the accuracy of processing network traffic and video stream data have improved. After the research, the authors select recurrent neural networks (RNN) as the primary model for training; next, discuss the analysis of recurrent neural networks (RNN) for handling temporal dependencies in network traffic and convolutional neural networks (CNN) for facial recognition from the organization database. The article presents the results of system testing, conducts computer simulations, and evaluates its effectiveness in detecting network threats and identifying suspicious objects in video data.*

Keywords: network traffic analysis, cyber threats, machine learning, convolutional neural networks, recurrent neural networks, video surveillance, facial recognition, information security

For citation: Filippova L.B., Leonov Yu.A., Martynenko A.A., Filippov R.A., Grin M.G. Automating Safety System Modelling in Organizations Using Neural Networks. Automation and modeling in design and management, 2025, no. 4 (30). pp. 24-32. doi: 10.30987/2658-6436-2025-4-24-32.

Введение

Анализ сетевого трафика организации является ключевым элементом обеспечения информационной безопасности. Традиционные методы выявления угроз основываются на сигнатурных подходах и эвристическом анализе, однако они не всегда эффективны при обнаружении сложных атак и аномального поведения в сети [1, 2]. Современные технологии машинного обучения позволяют автоматизировать этот процесс, повышая точность детектирования угроз.

В статье рассматривается применение нейросетевых моделей для анализа сетевого трафика. Используемая архитектура сочетает рекуррентные нейронные сети (*RNN*) для обработки временных зависимостей в данных и сверточные нейронные сети (*CNN*) для анализа изображений с систем видеонаблюдения. Такой подход позволяет выявлять аномальные сетевые активности и идентифицировать нарушителей по их лицам, сравнивая изображения с базой данных организации [3, 4].

Результаты тестирования данного подхода показали его эффективность в анализе сетевого трафика и распознавании изображений. Представленная система способна адаптироваться к изменяющимся условиям киберугроз и оперативно обнаруживать потенциально опасные события.

Материалы, модели, эксперименты и методы

Актуальные методы обеспечения информационной безопасности организаций включают в себя широкий спектр технологий для мониторинга сетевого трафика и обнаружения угроз. Одним из перспективных направлений в данной области является применение нейронных сетей, позволяющих анализировать большие объемы данных и выявлять аномалии в режиме реального времени [5].

В современном цифровом мире количество кибератак продолжает стремительно расти, что подтверждается статистическим отчетом «Ландшафт киберугроз за 2024» от Лаборатории Касперского (рис. 1).

Согласно данным отчета, зафиксировано более 1,2 миллиона инцидентов, что на 17 % больше по сравнению с предыдущим годом. Наибольшую угрозу представляют вредоносное ПО (26 %), фишинг (22 %), программы-вымогатели (18 %), а также *DDoS*-атаки (12 %) и эксплойты (10 %).

Статистические данные показывают, что методы атак становятся всё более изощрёнными: злоумышленники стараются замаскировать свои действия, а классические механизмы киберзащиты часто оказываются недостаточно эффективными [6, 7]. Это приводит к необходимости внедрения интеллектуальных решений, среди которых особое место занимают нейронные сети, способные анализировать сетевые процессы и фиксировать аномалии в момент их возникновения.

Одним из наиболее перспективных инструментов считаются рекуррентные нейронные сети (*RNN*), так как они умеют работать с временными последовательностями и выявлять нетипичные закономерности в сетевых коммуникациях [8, 9]. Их использование позволяет своевременно обнаруживать признаки кибератак. В то же время свёрточные нейронные сети (*CNN*)

находят применение в обработке визуальных данных – например, в задачах распознавания лиц с камер наблюдения, что помогает организациям противостоять не только виртуальным, но и физическим угрозам. Особенно остро такая защита необходима в госсекторе, финансовых и медицинских структурах, где кибератаки нередко направлены на получение критически важных данных [10, 11].

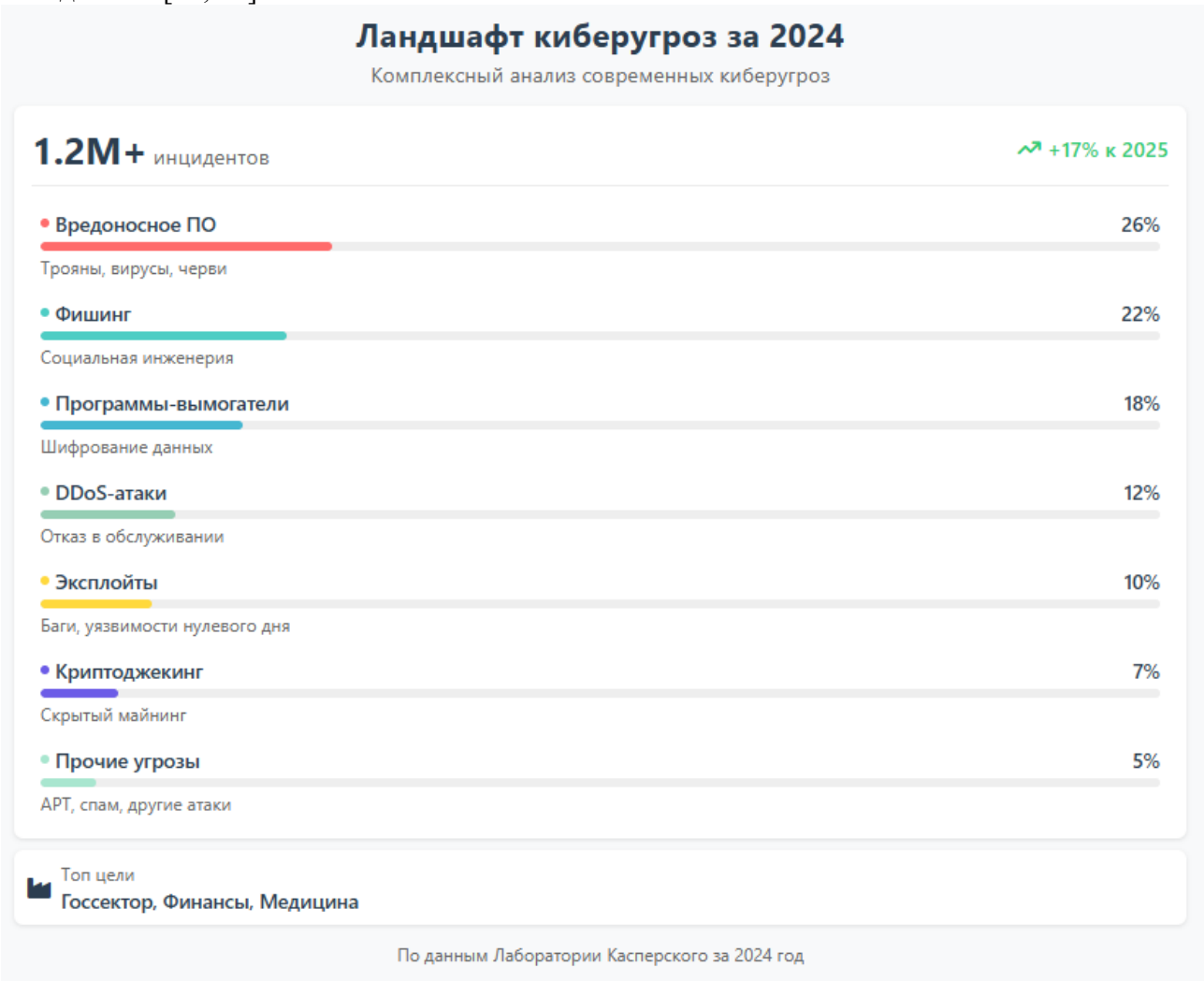

Рис. 1. Статистика киберугроз от Касперского за 2024 г
Fig. 1. Kaspersky cyber threat statistics for 2024

Таким образом, исследование возможностей *RNN* и *CNN* в обработке сетевого трафика и видеопотоков имеет высокую прикладную значимость. Эти технологии способны повысить уровень информационной безопасности за счёт автоматизированного выявления атак, что крайне важно в условиях роста количества инцидентов в киберпространстве.

Современные научные публикации подтверждают потенциал нейросетевых подходов. Так, *CNN* широко применяются для анализа изображений, а *RNN* – для выявления зависимостей во временных рядах и отслеживания аномального поведения пользователей. На практике всё чаще разрабатываются гибридные решения, объединяющие нейросетевые алгоритмы с традиционными средствами защиты, такими как *IDS* или *SIEM* [12]. Однако классические методы в основном используют сигнатурный анализ и нуждаются в постоянном обновлении баз, что ограничивает их применение для обнаружения новых, ранее неизвестных угроз. Нейросети же способны адаптироваться к меняющимся условиям и выявлять атаки без предварительного знания их сигнатур.

Результаты проведённого исследования показывают, что совмещение *RNN* и *CNN* повышает точность обработки как сетевого трафика, так и данных видеонаблюдения. В рамках работы предложена архитектура информационно-аналитической системы, включающая несколько модулей: блок обработки сетевых пакетов, компонент анализа видеопотоков и базу

данных для хранения информации о зафиксированных угрозах. Особое внимание при проектировании уделялось производительности и возможности интеграции с существующими средствами защиты.

Практическая ценность разработки заключается в том, что система способна функционировать в реальном времени, автоматически выявляя подозрительные действия и уведомляя службу безопасности. Такой подход позволяет минимизировать риски несанкционированного доступа и повысить оперативность реагирования на инциденты.

Для решения поставленных задач были исследованы 3 вида нейронных сетей: сверточные, рекуррентные и с долгой краткосрочной памятью.

Сверточные нейронные сети (CNN). CNN широко используются в задачах обработки визуальной информации, таких как изображение и видеоконтент. В нашей задаче требуется учитывать временные зависимости между данными сетевого трафика, а это затруднительно сделать с данной нейронной сетью.

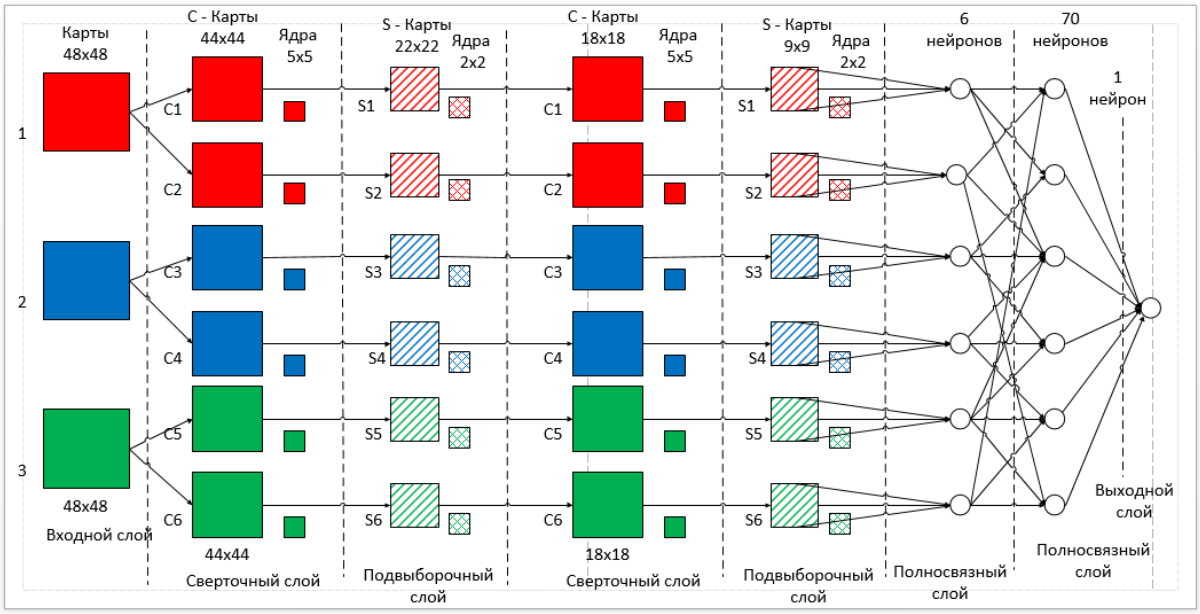

Рис. 2. Свёрточная нейронная сеть (*CNN*)
Fig. 2. Convolutional Neural Network (CNN)

Рекуррентные нейронные сети (RNN). RNN применяется для обработки информации, имеющую последовательную зависимую структуру, например, временные ряды, текст на естественном языке. Такое применение делает эти нейронные сети пригодными для использования в задачах анализа сетевого трафика (рис. 3).

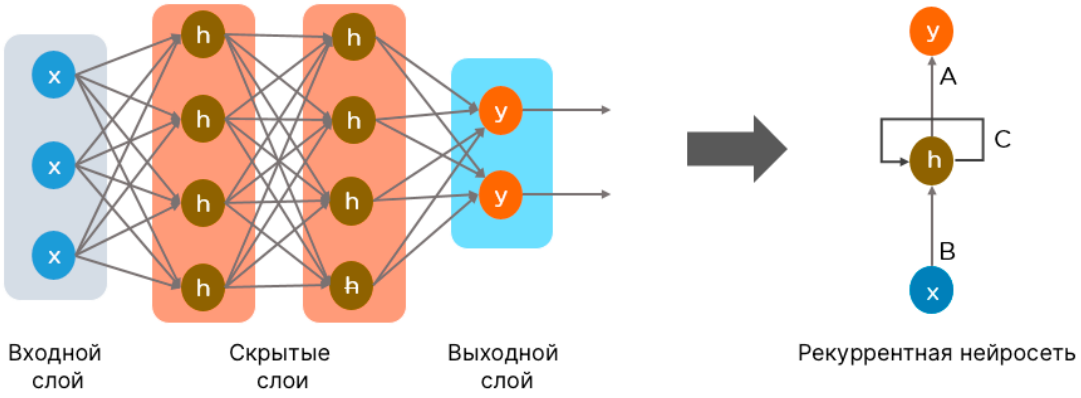

Рис. 3. Рекуррентная нейронная сеть (*RNN*)
Fig. 3. Recurrent neural network (RNN)

Сети с долгой краткосрочной памятью (LSTM). LSTM также может использоваться в задачах, где нужна память о структуре предыдущих данных, так как имеется возможность сохранять и учитывать на протяжении времени зависимости в ранее исследуемых данных (рис. 4). Однако применение этих сетей связано с использованием больших ресурсов по сравнению с *RNN* [3].

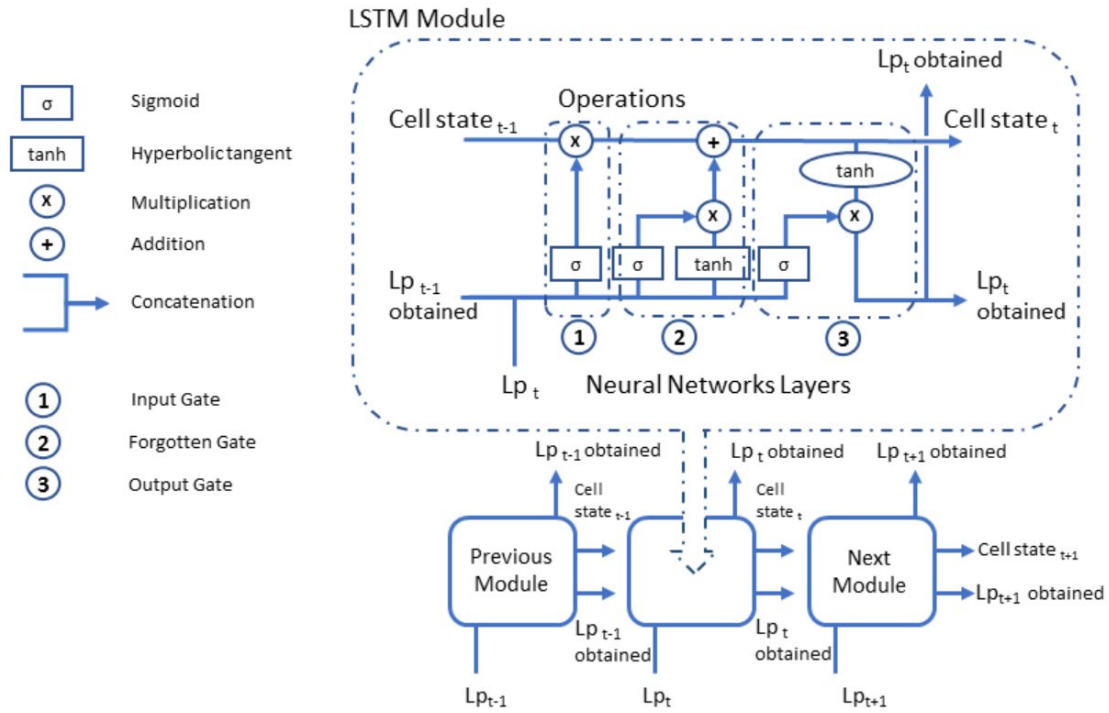

Рис. 4. Сеть с долгой краткосрочной памятью (*LSTM*)
Fig. 4. Long-term short-term memory Network (LSTM)

Для решения задачи анализа сетевого трафика была проведена проверка работы трёх архитектур нейронных сетей (рис. 5): рекуррентной (*RNN*), свёрточной (*CNN*) и сети с механизмом долгой краткосрочной памяти (*LSTM*). Сравнение осуществлялось по показателю точности выявления уязвимостей, который оценивался в зависимости от длины обрабатываемой последовательности пакетов.

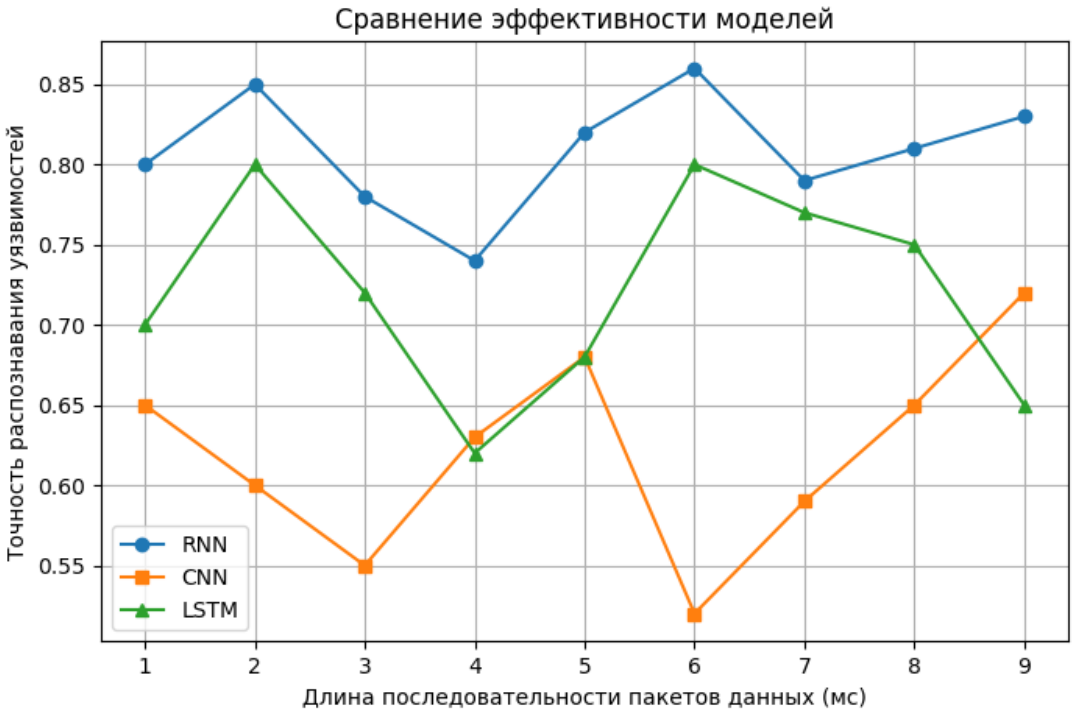

Рис. 5. Тестирование работы нейронных сетей для задачи анализа сетевого трафика
Fig. 5. Testing the operation of neural networks for the task of analyzing network traffic

Результаты, представленные на графике, показывают, что рекуррентная нейронная сеть (*RNN*) стабильно демонстрирует более высокую точность, чем свёрточные (*CNN*) и *LSTM*-сети, независимо от длины анализируемой последовательности. Особенно сильно разрыв за-

метен при работе с длинными сериями пакетов, где учёт последовательности и контекста играет ключевую роль. Именно поэтому применение *RNN* оказывается наиболее оправданным в задачах анализа сетевого трафика.

RNN использует предыдущую информацию, а это оптимально при поиске уязвимостей в сетевом обмене. Высокая результативность *RNN* объясняется тем, что анализ пакетов может выполняться при относительно небольших объёмах и коротких интервалах между поступающими данными, что делает эту архитектуру наиболее эффективной.

В ходе исследования были сопоставлены три модели – *CNN*, *RNN* и *LSTM* – на практическом примере (рис. 6).

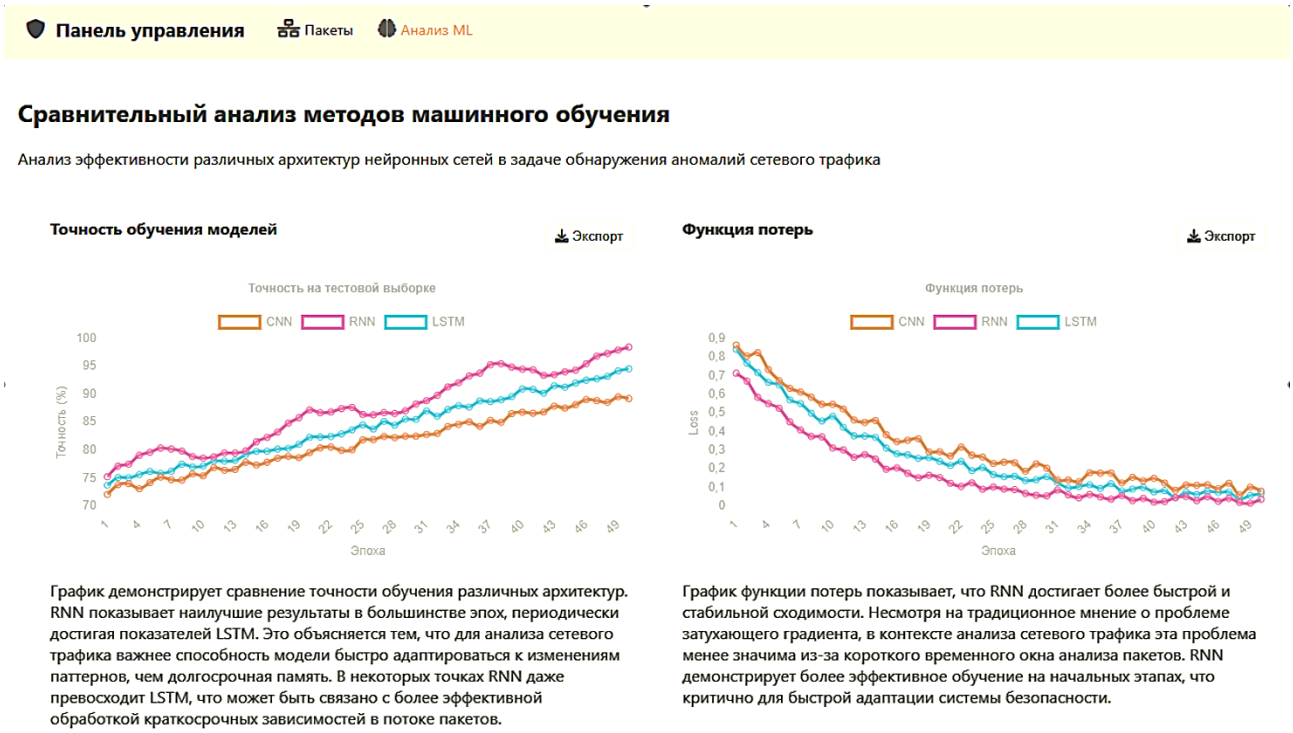

Рис. 6. Сравнение моделей в задаче анализа сетевого трафика
Fig. 6. Comparison of models in the task of network traffic analysis

График точности обучения демонстрирует превосходство архитектуры *RNN*, которая достигла наивысшей точности в 96,8 % на тестовой выборке. Это объясняется способностью *RNN* эффективно выявлять временные зависимости в данных сетевого трафика. *LSTM* показала немного более низкую точность – 95,2 %, а *CNN* – 92,5 %.

График функции потерь отражает процесс сходимости моделей. *RNN* демонстрирует наиболее стабильное снижение ошибки и достигает сходимости быстрее остальных архитектур. *LSTM* также показывает хорошую динамику, но в отдельных моментах сходится медленнее из-за высокой чувствительности к изменению паттернов. *CNN* демонстрирует быструю начальную сходимость, но раньше выходит на плато.

Исследование нейронных сетей с целью возможности применения в задаче анализа сетевого трафика показало:

– рекуррентные нейронные сети – получены самые высокие показатели, особенно по точности, полноте и *F*1-мере;

– сверточные нейронные сети – показали самые худшие результаты, однако время на обучение сети оказалось наименьшим;

– сети с долгой краткосрочной памятью – обеспечили высокую точность модели, однако потребовались большие трудозатраты с настройкой параметров, а также слишком много времени нужно на обучение модели.

Таким образом для задачи анализа сетевого трафика была выбрана рекуррентная нейронная сеть. Такая сеть будет эффективна в условиях появления новых видов угроз.

Процесс обучения рекуррентных нейронных сетей (*RNN*) является многокомпонентным и требует специальных подходов, позволяющих подстроить архитектуру под работу с времен-

ными последовательностями. Ключевая особенность *RNN* заключается в том, что они способны сохранять информацию между шагами обработки, что позволяет им выявлять закономерности во временных зависимостях данных.

Алгоритм обучения можно условно разделить на несколько этапов.

1. Начальная инициализация параметров.

Перед запуском обучения задаются значения весов сети. Это может выполняться как случайным образом, так и с применением специальных стратегий, улучшающих процесс сходимости.

2. Прямое распространение (*Forward pass*).

На каждом временном шаге t скрытое состояние обновляется с учётом текущего входного вектора x_t и состояния на предыдущем шаге h_{t-1}.

Состояние вычисляется по зависимости:

$$h_t = f(W_{hh}h_{t-1} + W_{xh}x_t + b_h), \quad (1)$$

где f – функция активации (*tanh*, *ReLU* и др.), W_{hh} – веса для рекуррентных связей, W_{xh} – веса, соединяющие входной слой со скрытым, b_h – смещение скрытого слоя.

3. Генерация выходного значения.

Для каждого временного шага результат работы сети определяется как:

$$y_t = g(W_{hy}h_t + b_y), \quad (2)$$

где g – функция активации выходного уровня, W_{hy} – веса между скрытым и выходным слоем, b_y – смещение выходного слоя.

После расчета выходов сети на всех временных шагах вычисляется ошибка (потеря) с помощью функции потерь (например, кросс-энтропия для задач классификации). Затем начинается обратное распространение ошибки (*BPTT*), в ходе которого градиенты ошибки распространяются обратно по сети для обновления весов. Важно отметить, что из-за рекуррентной природы *RNN* градиенты распространяются не только через слои сети, но и через временные шаги, что позволяет обновлять веса в соответствии с их влиянием на ошибку в разные моменты времени.

Основная проблема, с которой сталкиваются *RNN* при *BPTT* – это затухание или взрыв градиентов, когда градиенты становятся слишком маленькими или слишком большими для эффективного обучения. Описанные трудности решались стандартными подходами: обрезка градиентов и использование *LSTM* и *GRU*.

LSTM позволяет учитывать предыдущую информационную последовательность за счет дополнительных связей между скрытыми слоями цепочечных данных, однако невозможно управлять акцентами в предыдущих данных. Также со временем предыдущая информация «забывается». Такой проблемы можно избежать, применяя *GRU*.

GRU в отличие от *LSTM* использует взвешенные суммы, что позволяет ускорить процесс вычисления. Также *GRU* позволяет управлять «важностью» информации, т.е. можно указать какая информация очень важна и ее не стоит «забывать».

В данном научном исследовании использовались 3 вида задач: анализ сетевого трафика, обработка системных журналов, анализ видеоизображения.

1. Анализ сетевого трафика.

Анализировался входящий трафик на предмет возможных угроз. Применялись такие инструменты как *tcpdump* или *wireshark*.

С помощью *Python* и библиотеки *Pcapy* обрабатывались «*.pcap*-файлы», извлекались параметры: структура заголовков, *IP*-адреса источника и получателя, номера портов, а также содержимое передаваемых сообщений.

2. Обработка системных журналов.

Вторым источником информации стали логи операционной системы и событий пользователей. Анализировались следующие логи: /*var*/*log*/*syslog* и /*var*/*log*/*auth.log*, извлекались данные о запуске приложений, попытках входа в систему и изменениях конфигураций. Для фильтрации и выделения нужных событий применялись стандартные инструменты *Linux* (*grep*, *awk*, *sed*), позволяющие из больших объёмов текстовой информации выделять только релевантные записи.

3. Анализ видеоизображений.

Дополнительно использовались материалы с камер наблюдения. Видеопоток поступал

как от *IP*-камер, так и с локальных накопителей. Для его обработки применялись библиотеки *OpenCV* и *FFmpeg*: кадры преобразовывались в удобный для анализа вид (например, перевод в градации серого, повышение контрастности, вырезка области лица). Далее изображения передавались в нейросетевые модели (*CNN*) – архитектуры уровня *FaceNet* или *DeepFace*, что позволяло выполнять распознавание и идентификацию лиц. Для ускорения вычислений применялось аппаратное ускорение на графических процессорах (*CUDA*).

Результаты

В ходе исследования решались две задачи: выявление опасного сетевого трафика и распознавание лиц с камер видеонаблюдения.

Для задачи анализа сетевого трафика была выбрана рекуррентная нейронная сеть (*RNN*). Данная нейросетевая модель продемонстрировала высокую точность в анализе сетевого трафика и идентификации нарушителей по изображениям. В ходе работы были выявлен аномальный, нетипичный сетевой трафик, который требует отдельного анализа на предмет негативных угроз. Экспертная оценка такого трафика показывает точность выявления свыше 80 %.

Для задачи распознавания лиц с камер видеонаблюдения была выбрана сверточная нейронная сеть (*CNN*). Была проведена предварительная подготовка видеопотока: разбивка на отдельные изображения и выбор из них наиболее информативного, перевод изображения в градацию серого с повышением контрастности (упрощение изображения), выявление на изображении отдельных лиц. Далее нейронная сеть обучалась на подготовленных примерах (около 500). Построенная модель дает точность распознавания свыше 95 %.

Полученные результаты можно использовать в реальных организациях для повышения их информационной безопасности. Планируется продолжить работу в данном направлении. Необходимо улучшать качество моделей и алгоритмов, используемых в работе.

Заключение

В ходе работы была подтверждена эффективность использования нейросетевых моделей для задач, связанных с обеспечением информационной безопасности организации.

В качестве новизны можно отметить объединение в единую инфраструктуру результатов анализа сетевого трафика и анализа видеоизображений, полученных с камеры видеонаблюдения. При этом использовались нейронные сети различных видов. Используемый подход позволяет внедрить комплексную систему защиты, включающую выявление опасных событий в сетевом и визуальном информационных потоках. Рекуррентная нейронная сеть обучена с точностью около 96 % и позволяет качественно выявлять угрозы в сетевом трафике. Сверточная нейронная сеть с точностью около 95 % успешно выявляет лиц незарегистрированных в базе данных, а следовательно, могут являться потенциальными нарушителями.

Практическая ценность данной работы составляют разработанные программные модули, которые при желании можно внедрить в существующей организации без необходимости перестраивать сложившиеся принципы работы.

Таким образом проведенное научное исследование и программная реализация теоретических наработок вносит необходимый вклад в развитие технологий, повышающих безопасность работы организаций.

Список источников:

1. Краснопольский Б.М. Введение в анализ данных и машинное обучение. – М.: Изд-во Юрайт, 2020. – 310 с.

2. Законов А.П. Анализ больших данных в системах искусственного интеллекта. – Санкт-Петербург: Питер, 2021. – 342 с.

3. Колесников А.В., Кроль Д.А. Методы оптимизации в машинном обучении. – М.: Физматлит, 2022. – 390 с.

4. Левенштейн В.И. Алгоритмы, машины и люди: обработка языка, зрения и разума // М.: Наука, 2019. – 301 с.

5. Смирнов И.А. Интеллектуальный анализ данных: Теория и практика // М.: Бином. Лаборатория знаний, 2021. – 452 с.

References:

1. Krasnopolsky B.M. Introduction to Data Analysis and Machine Learning. Moscow: Yurayt; 2020.

2. Zakonov A.P. Big Data Analysis in Artificial Intelligence Systems. Saint Petersburg: Piter; 2021.

3. Kolesnikov A.V., Krol D.A. Optimization Methods in Machine Learning. Moscow: Fizmatlit; 2022.

4. Levinstein V.I. Algorithms, Machines, and People: Language, Vision, and Mind Processing. Moscow: Nauka; 2019.

5. Smirnov I.A. Intelligent Data Analysis: Theory and Practice. Moscow: BINOM. Laboratoriya znaniy; 2021.

6. Петровский А.Б. Методы и модели искусственного интеллекта // Москва: Интернет-Уни-верситет Информационных Технологий, 2022. – 341 с.

7. Горбунова И.П., Орлов П.А. Современные технологии машинного обучения. – М.: Академия, 2022. – 377 с.

8. Разработка математической модели информационной системы для инвентаризации и мониторинга программного и аппаратного обеспечения на основе методов нечеткой логики / Р.А. Филиппов, Л.Б. Филиппова, А.В. Аверченков [и др.] // Качество. Инновации. Образование. – 2018. – № 7(158). – С. 105-112.

9. Исследование операций: Лабораторный практикум / Ю.А. Леонов, Е.А. Леонов и др. – М.: Общество с ограниченной ответственностью «ФЛИНТА», 2018. – 94 с.

10. Филиппов Р.А., Филиппова Л.Б., Леонов Ю.А. Применение микроконтроллера arduino mega 2560 для автоматизации работы микроскопа LEICA DM IRM // Автоматизация и моделирование в проектировании и управлении. – 2021. – С. 210-213.

11. Прогнозирование оттока клиентов телекоммуникационной компании на основе метода опорных векторов / Ю.А. Леонов, Н.С. Дьячков и др. // Известия Тульского государственного университета. Технические науки. – 2022. – № 7. – С. 228-234.

12. Development of an information and analytical system for modeling the demographic situation in the Russian Federation / D.R. Kalugin, Yu.A. Leonov et al. // III International Workshop on Modeling, Information Processing and Computing (MIP: Computing-2021), Krasnoyarsk, 28 мая 2021 года. Vol. 2899. – Krasnoyarsk, Russia: CEUR-WS, 2021. – P. 133-140.

6. Petrovsky A.B. Methods and Models of Artificial Intelligence. Moscow: INTUIT; 2022.

7. Gorbunova I.P., Orlov P.A. Modern Machine Learning Technologies. Moscow: Akademia; 2022.

8. Filippov RA, Filippova LB, Averchenkov AV, et al. Development of a Mathematical Model of an Information System for Inventory and Monitoring of Software and Hardware Based on Fuzzy Logic Methods. Quality. Innovation. Education. 2018;7(158):105-112.

9. Leonov YA, Leonov EA, et al. Laboratory Workshop on Operations Research. Moscow: Flinta; 2018.

10. Filippov RA, Filippova LB, Leonov YA, et al. Application of the Arduino Mega 2560 Microcontroller for Automation of the LEICA DM IRM Microscope. In: Proceedings of the All-Russian Conference on Automation and Modelling in Design and Management; 2021 May 19; Bryansk: BSTU; 2021. p. 210-213.

11. Leonov YA, Dyachkov NS, et al. Forecasting the Outflow of Customers of a Telecommunications Company Based on the Support Vector Method. Izvestiya Tula State University. 2022;7:228-234.

12. Kalugin DR, Leonov YuA, et al. Development of an Information and Analytical System for Modelling the Demographic Situation in the Russian Federation. In: Proceedings of the 3rd International Workshop on Modelling, Information Processing and Computing MIP: Computing-2021; 2021 May 28; Krasnoyarsk: CEUR-WS: 2021; vol. 2899. p. 133-140.

Информация об авторах:

Филиппова Людмила Борисовна
кандидат технических наук, доцент Брянского государственного технического университета.

Леонов Юрий Алексеевич
кандидат технических наук, доцент Брянского государственного технического университета.

Мартыненко Алексей Александрович
кандидат технических наук, доцент Брянского государственного технического университета.

Филиппов Родион Алексеевич
кандидат технических наук, доцент Брянского государственного технического университета.

Гринь Марина Георгиевна
кандидат экономических наук, доцент Брянского государственного технического университета.

Information about the authors:

Filippova Lyudmila Borisovna
Candidate of Technical Sciences, Associate Professor of Bryansk State Technical University

Leonov Yuri Alekseevich
Candidate of Technical Sciences, Associate Professor of Bryansk State Technical University

Martynenko Alexey Alexandrovich
Candidate of Technical Sciences, Associate Professor of Bryansk State Shock Technical University

Filippov Rodion Alekseevich
Candidate of Technical Sciences, Associate Professor of Bryansk State Technical University

Grin Marina Georgievna
Candidate of Economic Sciences, Associate Professor of Bryansk State Technical University

Вклад авторов: все авторы сделали эквивалентный вклад в подготовку публикации.
Contribution of the authors: the authors contributed equally to this article.

Авторы заявляют об отсутствии конфликта интересов.
The authors declare no conflicts of interests.

Статья поступила в редакцию 01.10.2025; одобрена после рецензирования 06.11.2025.2025; принята к публикации 07.11.2025.

The article was submitted 01.10.2025; approved after reviewing 06.11.2025.2025; accepted for publication 07.11.2025.

Рецензент – Малаханов А.А., кандидат технических наук, доцент, Брянский государственный технический университет.

Reviewer – Malakhanov A.A., Candidate of Technical Sciences, Associate Professor, Bryansk State Technical University.