СОВРЕМЕННЫЕ ТЕНДЕНЦИИ В НАУКЕ, ИСКУССТВЕ И ТЕХНОЛОГИИ: МЕЖДИСЦИПЛИНАРНЫЕ ПЕРСПЕКТИВЫ

СБОРНИК НАУЧНЫХ ТРУДОВ

www.scipro.ru

НАУЧНАЯ ОБЩЕСТВЕННАЯ ОРГАНИЗАЦИЯ
ПРОФЕССИОНАЛЬНАЯ НАУКА

Сборник научных трудов по материалам Международной научно-практической конференции «Современные тенденции в науке, искусстве и технологии: междисциплинарные перспективы»

10 апреля 2025г.

www.scipro.ru
Краснодар, 2025

УДК 009
ББК 6/8

Главный редактор: Н.А. Краснова
Технический редактор: Ю.О.Канаева

Сборник научных трудов по материалам Международной научно-практической конференции «Современные тенденции в науке, искусстве и технологии: междисциплинарные перспективы», 10 апреля 2025 г., Краснодар: Профессиональная наука, 2025. – 20 с.

ISBN 978-1-326-51598-0

В сборнике научных трудов рассматриваются актуальные вопросы развития экономикики, политологии, граждановедения, юриспруденции и т.д. по материалам Международной научно-практической конференции «Современные тенденции в науке, искусстве и технологии: междисциплинарные перспективы, состоявшейся 10 апреля 2025 г. в г. Краснодар.

Сборник предназначен для научных и педагогических работников, преподавателей, аспирантов, магистрантов и студентов с целью использования в научной работе и учебной деятельности.

Все включенные в сборник статьи прошли научное рецензирование и опубликованы в том виде, в котором они были представлены авторами. За содержание статей ответственность несут авторы.

Электронная версия сборника находится в свободном доступе на сайте www.scipro.ru.

При верстке электронной книги использованы материалы с ресурсов: PSDgraphics

УДК 009

ББК 6/8

СОДЕРЖАНИЕ

СЕКЦИЯ 1. ГЛОБАЛЬНАЯ ЭКОНОМИКА И МАКРОЭКОНОМИЧЕСКИЕ ТРЕНДЫ: ВЫЗОВЫ И ПЕРСПЕКТИВЫ

УДК 338.45

Тихонов В.Д. Энергетическая безопасность и экономика: вызовы для топливно-энергетического комплекса Республики Беларусь

Energy security and economy: challenges for the fuel and energy complex of the Republic of Belarus

Тихонов Виктор Даниилович,
Магистрант,
Белорусский государственный экономический университет
Научный руководитель
Ананенко Н.С., к. э. н., доцент кафедры финансов,
Белорусский государственный экономический университет
Tikhonov Victor Daniilovich,
Master's student,
Belarusian State Economic University
Scientific advisor: Ananenko N.S.,
Candidate of Economic, Associate Professor of Finance Department,
Belarusian State Economic University

Аннотация. *В статье рассмотрены актуальные проблемы функционирования топливно-энергетического комплекса Республики Беларусь: перекрестное субсидирование, разбалансированность тарифного регулирования, а также высокая импортозависимость от внешних поставщиков энергоресурсов. Предложены меры по реформированию системы регулирования, оптимизации расходов и диверсификации источников энергоснабжения для обеспечения энергетической безопасности страны.*

Ключевые слова: *энергетика, топливно-энергетический комплекс, энергетическая безопасность, перекрестное субсидирование, энергоресурсы, тарифное регулирование.*

Abstract. *The article discusses the current problems of the functioning of the fuel and energy complex of the Republic of Belarus, such as cross-subsidization, imbalance of tariff regulation, as well as high import dependence on external energy suppliers. Measures have been proposed to reform the regulatory system, optimize costs and diversify energy supply sources to ensure the country's energy security.*

Keywords: *energy, fuel and energy complex, energy security, cross-subsidization, energy resources, tariff regulation.*

Топливно-энергетический комплекс Республики Беларусь представляет собой совокупность отраслей, связанных с производством и распределением энергии в различных её видах и формах [1, с. 8]. Для экономики он является одним из ключевых комплексов, в котором концентрируется огромное количество трудовых и материальных ресурсов. Производимая им продукция используется во всех видах деятельности, начиная от промышленности и заканчивая жилищно-коммунальным хозяйством. Значимость топливно-

энергетического комплекса трудно переоценить, поскольку его стабильное функционирование является основой энергетической безопасности и устойчивого экономического развития страны. Несмотря на ключевую роль топливно-энергетического комплекса в экономике, его развитие сопровождается рядом сложностей, требующих своевременного реагирования. Рассмотрим основные проблемы, с которыми сталкивается топливно-энергетический комплекс, и возможные пути их решения:

1. Наличие перекрестного субсидирования. В настоящее время тарифы на электрическую и тепловую энергию для населения устанавливаются Советом Министров Республики Беларусь на уровне ниже базовых тарифов. Недополученная в связи с этим выручка организаций топливно-энергетического комплекса подлежит компенсации за счет установления более высоких тарифов на электрическую и тепловую энергию для других групп потребителей [2]. В свою очередь это приводит к увеличению затрат на производство продукции, работ, услуг, и снижает конкурентоспособность продукции отечественных производителей по ценовому фактору.

По нашему мнению, практику перекрестного субсидирования необходимо совершенствовать. По мере роста реальных доходов населения целесообразно снижать объем перекрестного субсидирования. Одновременно следует предусмотреть возможность предоставления за счет бюджетных средств адресной помощи отдельным категориям граждан.

2. Разбалансированность тарифного регулирования на разных уровнях: изменение стоимости природного газа (в сторону увеличения) не всегда приводит к соответствующей корректировке тарифов на электрическую и тепловую энергию для отдельных групп потребителей. В данном случае энергоснабжающие организации ГПО «Белэнерго» получают доход, который не позволяет им в полном объеме покрывать произведенные затраты. Это приводит к возникновению убытков у данных организаций, ухудшает их финансовое состояние. В Республике Беларусь решающее значение в регулировании данной сферы принадлежит Правительству страны. В последние годы сложилась практика, когда все решения по установлению тарифов на энергоресурсы принимаются на заседании Президиума Совета Министров, совещаниях в Совете Министров. И, как правило, решение принимается в пользу потребителей реального сектора экономики (сохранение тарифов) с целью обеспечения их конкурентоспособности на внешних рынках.

С учетом изложенного предлагается создать в Республике Беларусь независимый регулирующий орган с подчинением его напрямую Президенту Республики Беларусь. На первоначальном этапе предлагается передать указанному органу функции регулирования цен (тарифов) на природный и сжиженный газ, электрическую и тепловую энергию с

последующей передачей регулирования всех видов жилищно-коммунальных услуг, оказываемых населению.

3. Включение в себестоимость производства энергии затрат, нехарактерных для электроэнергетической отрасли. К таким затратам, прежде всего, относятся расходы на финансирование спортивных клубов, сельскохозяйственных структурных подразделений, объектов социальной инфраструктуры. Кроме того, в соответствии Указом Президента Республики Беларусь от 1 июля 2005 г. № 300 «О предоставлении и использовании безвозмездной (спонсорской) помощи» и Указом Президента Республики Беларусь от 15 апреля 2013 г. № 191 «Об оказании поддержки организациям физической культуры и спорта» за счет прибыли энергоснабжающих организаций оказывается финансовая поддержка футбольным и хоккейным клубам в размерах, устанавливаемых местными исполнительными и распорядительными органами власти [3, 4].

Исключение из себестоимости производства и реализации энергии энергоснабжающих организаций таких расходов является обоснованным. Это позволит улучшить их финансовое состояние и не допустить прирост соответствующих тарифов на энергию для потребителей реального сектора экономики.

4. В условиях ограниченности собственной ресурсной базы, актуальными являются проблемы энергетической безопасности республики. Проблема обусловлена тем, что Республика Беларусь приобретает более 80 % топлива за границей (преимущественно у Российской Федерации) [5]. К прочим угрозам также относится повышение цен на импортируемые топливные ресурсы, отказ от импорта либо его ограничение сопредельными странами, дискриминационные действия на внешних рынках по отношению к экспортируемым товарам и услугам отраслей ТЭК.

Важнейшими направлениями и мерами по обеспечению экономической безопасности в энергетической сфере являются: повышение уровня обеспеченности энергией за счет собственных источников путем стимулирования использования местных энергоресурсов; диверсификация поставщиков и видов энергоресурсов; повышение экономической эффективности производства и распределения энергии за счет модернизации и устаревших основных производственных фондов ТЭК.

Решение перечисленных выше проблем позволит повысить финансовую устойчивость и эффективность работы организаций топливно-энергетического комплекса, обеспечив его стабильное развитие в долгосрочной перспективе.

Библиографический список

1. Зылёва, Н.В. Учет в нефтегазодобывающей отрасли : учебник и практикум для вузов / Н.В. Зылёва, Е.Г. Токмакова, Ю.С. Сахно. – 2-е изд. – М. : Юрайт, 2022. – 205 с.

2. Об утверждении Положения о порядке формирования цен (тарифов) на природный и сжиженный газ, электрическую и тепловую энергию : Постановление Совета Министров Респ. Беларусь, 17 марта 2014 г., № 222 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2025.

3. О предоставлении и использовании безвозмездной (спонсорской) помощи : Указ Президента Респ. Беларусь, 1 июля 2005 г., № 300 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2025.

4. Об оказании поддержки организациям физической культуры и спорта : Указ Президента Респ. Беларусь, 15 апреля 2013 г., № 191 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2025.

5. Рябцева, Л.А. Топливно-энергетический комплекс Республики Беларусь: проблемы и перспективы развития [Электронный ресурс] / Л.А. Рябцева // Электронная библиотека БГУ. – Режим доступа: https://elib.bsu.by/bitstream/123456789/114820/1/raybtseva_sbornik14.pdf. – Дата доступа: 16.03.2025.

СЕКЦИЯ 2. МЕЖДИСЦИПЛИНАРНЫЕ ПОДХОДЫ В ИСКУССТВЕ И НАУКЕ: НОВЫЕ ФОРМЫ ВЗАИМОДЕЙСТВИЯ

УДК 004.738.5

Воробьев П.В., Москалев В.С. Перспективы использования SDR в архитектуре Интернета вещей

Prospects of using SDR in the architecture of the Internet of Things

Воробьев Павел Владимирович,
Младший научный сотрудник,
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Москалев Владимир Сергеевич,
Слушатель,
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Vorobyev Pavel Vladimirovich,
Junior researcher,
Military academy of telecommunications
Moskalev Vladimir Sergeevich,
Student,
Military academy of telecommunications

Аннотация. *С развитием IoT возрастает потребность в гибких и энергоэффективных решениях для беспроводной связи. SDR открывает новые возможности для IoT-архитектур, позволяя динамически адаптировать параметры радиопередачи под различные сценарии использования. В статье рассматриваются ключевые преимущества SDR для IoT и анализируются проблемы внедрения. Приведены некоторые примеры использования SDR в IoT.*
Ключевые слова: *Интернет вещей, IoT, SDR, программно-конфигурируемое радио*
Abstract. *With the development of the IoT, the need for flexible and energy-efficient wireless communication solutions is increasing. SDR opens up new possibilities for IoT architectures, allowing you to dynamically adapt radio transmission parameters to different usage scenarios. The article discusses the key advantages of SDR for IoT and analyzes the problems of implementation. Some examples of using SDR in IoT are given.*
Keywords: *Internet of Things, IoT, SDR, Software Defined Radio*

Современный Интернет Вещей (IoT) стремительно развивается, объединяя миллионы устройств — от умных датчиков до целых систем промышленного комплекса. Однако традиционные подходы к передаче данных часто сталкиваются с ограничениями по гибкости, энергоэффективности или совместимости. В этом контексте технология программно-определяемого радио (SDR) открывает новые перспективы, позволяя динамически адаптировать радиопараметры под различные IoT-сценарии.

SDR обеспечивает возможность гибкой настройки радиоинтерфейсов, что особенно важно для IoT-архитектур, где требуется одновременная поддержка множества стандартов

связи (LoRa, Zigbee, NB-IoT и др.) и работа в условиях меняющейся радиочастотной среды. Внедрение SDR может повысить масштабируемость, снизить энергопотребление и упростить интеграцию новых протоколов без замены аппаратного обеспечения.

В данной статье рассматриваются ключевые преимущества использования SDR в IoT, а также потенциальные направления развития этой технологии в контексте умных городов, промышленного IoT и других прикладных областей.

SDR — это технология, в которой традиционные аппаратные компоненты радиосистем (фильтры, модуляторы, демодуляторы) заменяются программными алгоритмами. Это позволяет гибко настраивать параметры радиопередачи (частоту, модуляцию, протоколы) без изменений в конфигурации физического оборудования.

В сфере IoT, где устройства часто работают одновременно в сетях различных стандартов (LPWAN, Wi-Fi, Bluetooth, Zigbee и др.), SDR может стать универсальным решением для: динамического переключения между протоколами (например, адаптация к зашумленному эфиру), уменьшения аппаратной сложности (одним модулем SDR возможно решать несколько задач параллельно), повышения энергоэффективности за счет оптимизации параметров передачи.

SDR позволяет IoT-устройствам автоматически выбирать оптимальный протокол связи в зависимости от условий. Так, в городской среде с высокой загрузкой спектра устройство SDR способно постоянно сканировать спектр и переключаться на менее зашумленные участки. Также контроллер SDR позволяет реализовывать несколько стандартов связи в одном блоке. Пример: Датчик в умном городе может использовать LoRa для дальних передач с низким энергопотреблением, но при необходимости переключиться на Wi-Fi для передачи больших объемов данных. Тем самым SDR позволяет заменить несколько радиомодулей единой программируемой платформой, снижая затраты на производство и обслуживание.

По мере развития IoT появляются новые протоколы (например, MIoTy, Wi-SUN, Matter). SDR позволяет обновлять использовать их с помощью обновления программного обеспечения, тем самым, позволяя избегать покупки нового дорогостоящего оборудования. Несмотря на преимущества, использование SDR в IoT сталкивается с некоторыми проблемами.

Обработка радиосигналов в реальном времени требует мощных процессоров, что может быть проблемой для маломощных IoT-устройств. Решением может послужить использование специализированных SDR-чипов с низким энергопотреблением (например, на базе RISC-V).

Также, программируемость радиоканала делает SDR-устройства уязвимыми к атакам на физическом уровне (глушение, подмена сигнала). Для более безопасного

использования таких систем требуются криптографические методы защиты и механизмы обнаружения действий нарушителей.

Динамическое переключение диапазонов необходимо использовать с осторожностью, т.к. в Российской Федерации существует строгое распределение частотного спектра по соответствующим службам, возможно, потребуется дополнительная сертификация.

SDR в сочетании с искусственным интеллектом может реализовывать когнитивное радио, где устройства самостоятельно анализируют эфир и выбирают оптимальные параметры связи.

Так в [1] описан вариант применения SDR для обеспечения работающей сотовой сети. В Чаде, где 80% населения живёт за счёт натурального хозяйства, сельское хозяйство сталкивается с огромными трудностями — засухи, нехватка воды, сложные климатические условия. Авторы описывают, как современные технологии могут помочь фермерам в самых отдалённых и засушливых регионах. Всё начинается с датчиков Интернета вещей, которые собирают данные о влажности почвы, температуре и других ключевых показателях. Для этого используется протокол MQTT — он эффективно работает даже при ограниченной пропускной способности. Здесь на помощь приходит SDR-технология — достаточно гибкая, чтобы иметь возможность адаптироваться под доступные частоты. Всё это интегрируется в платформу Fledge, где получаемые данные передаются в систему, где, по ним, составляются соответствующие рекомендации для фермеров.

В ходе тестов решение показало впечатляющую скорость передачи данных — 37,94 Мб/с, что доказывает его работоспособность даже в сложных условиях.

В [2] разработчики из США представляют собственное SDR решение для использования
в IoT платформах – tinySDR (рисунок 1). Эта SDR-система, специально разработана для энергоограниченных IoT-устройств. Данная система позволяет решить некоторые проблемные вопросы, связанные с применением SDR в IoT.

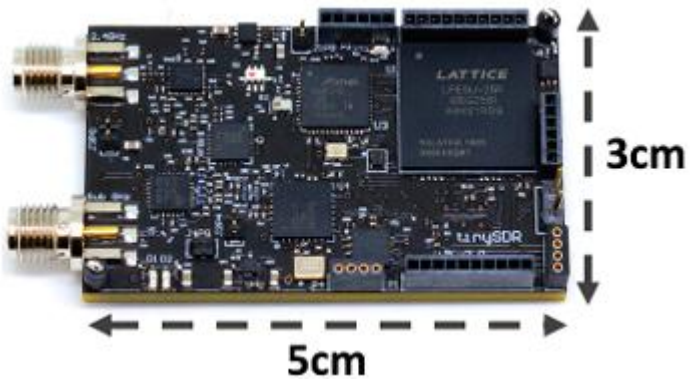

Рисунок 1. Платформа tinySDR

Она обеспечивает полностью автономную архитектуру с возможностью цикличной работы от батарей, что характерно для IoT-устройств. Также данная система поддерживает беспроводной доступ к программному модулю, что позволяет обеспечивать контроль обновления в удаленном формате.

Платформа была всесторонне протестирована с реализацией двух популярных IoT-протоколов: реализация протокола LoRa продемонстрировала чувствительность -126 дБм при использовании 11% ресурсов FPGA, реализация BLE-маяков показала чувствительность -94 дБм при загрузке всего 3% FPGA.

Особый научный интерес представляет исследование возможности демодуляции множественных одновременных передач LoRa в реальном времени в условиях жестких энергетических и вычислительных ограничений IoT-устройств. Экспериментальные результаты подтвердили осуществимость данной задачи на предложенной платформе.

Таким образом, разработанная tinySDR-платформа предоставляет исследователям мощный и многофункциональный инструмент для прототипирования IoT-протоколов, позволяет проводить полевые испытания новых решений в реалистичных условиях при низких затратах

Полученные результаты свидетельствуют о высокой эффективности предложенного подхода и его перспективности для дальнейших исследований в области энергоэффективных беспроводных технологий.

В [3] исследуется подход к беспроводной синхронизации времени для IoT-устройств на основе гибридной архитектуры TCR-SDR. Предлагаемое решение сочетает стандартные функции беспроводной связи IoT-устройств с дополнительными возможностями точной временной синхронизации и измерения расстояний за счет интеграции обычного IoT-трансивера со стабильным источником тактовой частоты и I/Q-трансивером, реализованными на базе ПЛИС и микроконтроллера. Экспериментальная платформа TCR-SDR в форм-факторе Receiver Carrier Board взаимодействует с OCP-TAP Time Card, использующей GNSS-приемник и резервный источник времени, при этом в качестве транспортного протокола применяется LoRa.

Исследование фокусируется на оценке пределов точности синхронизации для TCR-SDR и анализе возможностей распределения референсных сигналов 10 МГц и 1 PPS между устройствами. Полученные результаты демонстрируют перспективность предложенного подхода для создания масштабируемых систем временной синхронизации в IoT-сетях без ущерба для основных функций беспроводной связи. Разработанная архитектура открывает новые возможности для интеграции IoT-устройств с системами точного времени, что особенно актуально для приложений, требующих согласованной работы распределенных беспроводных сенсорных сетей.

Заключение

SDR обладает значительным потенциалом для IoT, предлагая гибкость, энергоэффективность. Однако широкое внедрение требует решения проблем с вычислительной сложностью, безопасностью и регулированием.

В ближайшие годы можно ожидать появления специализированных SDR-решений для IoT — энергоэффективных, защищенных и поддерживающих AI-оптимизацию радиопараметров. Это сделает SDR ключевой технологией для масштабируемых и адаптивных IoT-сетей.

Библиографический список

1. D. Fatimatou, M. Ba, T. Kondengar and S. Ouya, "SMART-AGRI-TCHAD: An Integrated IoT-SDR Architecture for Smart Agriculture in Arid Zones," 2024 International Conference on Intelligent Communication, Sensing and Electromagnetics (ICSE), Guangzhou, China, 2024, pp. 83-88,

2. M. Hessar, A. Najafi, V. Iyer, S. Gollakota, "TinySDR: Low-Power SDR Platform for Over-the-Air Programmable IoT Testbeds", 17th USENIX Symposium on Networked Systems Design and Implementation, Santa Clara, CA, USA, 2020.

3. W. Myrick, N. Shiga, J. S. James and A. Byagowi, "Timing, Communications, and Ranging SDR (TCR-SDR) for IoT Wireless Synchronization," 2024 IEEE International Symposium on Precision Clock Synchronization for Measurement, Control, and Communication (ISPCS), Tokyo, Japan, 2024, pp. 1-7

УДК 004.852

Задбоев В.А. Обучение нейросети на основе метода Байеса для предсказания внешних вторжений

Training a Bayesian neural network to predict external intrusions

Задбоев Вадим Александрович,
Младший научный сотрудник научно-исследовательского центра
Военной академии связи им. С.М. Буденного
Zadboev Vadim Aleksandrovich,
Junior research fellow of the research center
of the Military Academy of Communications named after S.M. Budyonny

Аннотация. *В статье рассматривается процесс создания набора данных для обучения нейросети, предсказывающей вторжения на основе метода Байеса. Подробно описываются этапы сбора, предобработки и аннотации данных, а также интеграция байесовского подхода в модель машинного обучения. Особое внимание уделяется важности качественных данных и их влиянию на точность прогнозирования аномалий. Представленные методы позволяют повысить эффективность систем обнаружения кибератак.*

Ключевые слова: *метод Байеса, нейросети, набор данных, обнаружение вторжений, кибербезопасность, предобработка данных, машинное обучение, сетевой трафик, аномалии, прогнозирование атак*

Abstract. *The article discusses the process of creating a dataset for training a neural network that predicts intrusions based on the Bayesian method. The stages of data collection, preprocessing, and annotation are described in detail, as well as the integration of the Bayesian approach into machine learning models. Particular attention is paid to the importance of high-quality data and its impact on anomaly prediction accuracy. The presented methods improve the efficiency of cyberattack detection systems.*

Keywords: *Bayesian method, neural networks, dataset, intrusion detection, cybersecurity, data preprocessing, machine learning, network traffic, anomalies, attack prediction*

В современном мире кибербезопасность становится одной из ключевых задач для компаний и организаций. Для защиты информационных систем от атак злоумышленников всё чаще применяются технологии машинного обучения и искусственного интеллекта. Одним из популярных подходов является использование байесовских методов для анализа сетевого трафика и выявления аномалий, которые могут указывать на попытки несанкционированного доступа.

Перед началом исследования определим базовые понятия.

Метод Байеса – это статистический подход, позволяющий оценивать вероятность того, что событие произошло при наличии определённых наблюдений. В контексте кибербезопасности этот метод используется для анализа сетевого трафика и выявления аномалий, которые могут быть признаками атаки.

Формула Байеса выглядит следующим образом:

$$P(A|B) = \frac{P(B|A)*P(A)}{P(B)} \quad (1)$$

где:

$P(B|A)$ – вероятность события A при условии, что произошло событие B,

$P(B|A)$ – вероятность события B при условии, что произошло событие A,

$P(A)$ и $P(B)$ – безусловные вероятности событий *A* и *B* соответственно.

Нейросеть представляет собою математическую модель, способную обучаться на больших объёмах данных и находить сложные зависимости между входными и выходными параметрами. В задачах кибербезопасности нейросети часто используются для классификации трафика или предсказания атак.

Для успешного обучения нейросети, предсказывающей вторжения, необходимо создать качественный набор данных. Алгоритм представлен на рисунке 1.

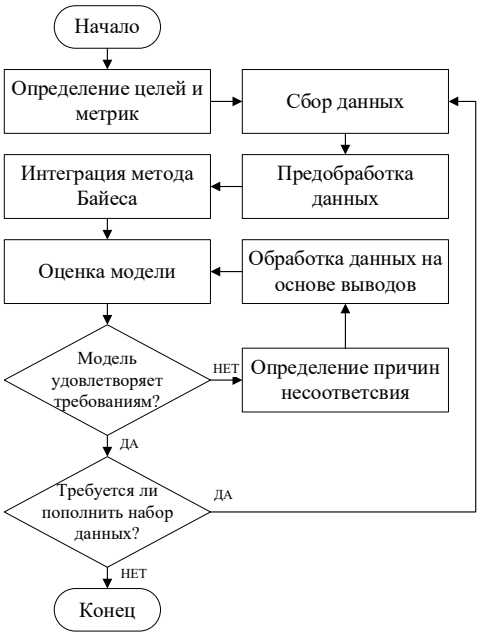

Рисунок 1. Алгоритм обучения нейросети

Перед началом сбора данных важно чётко определить цели проекта. Например, какие типы атак нужно выявлять (*DDoS*-атаки, сканирование сети, эксплуатация уязвимостей) и какие будут использоваться метрики для оценки эффективности созданной модели (точность, полнота, *F*1-мера).

На этапе сбора данных первоначально разграничиваются «нормальные» и «аномальные» данные, а также выбираются источники данных, например:

– логи серверов и сетевого оборудования;

– генерация искусственных данных о потенциальных атаках;

– использование открытых датасетов (*KDD Cup* 1999, *NSL-KDD*, *CICIDS*2017), содержащие информацию о нормальной и аномальной активности.

Наиболее необходимыми данными являются:

– *IP*-адреса и порты источника;

– протоколы соединений (*TCP*, *UDP*, *ICMP*) и длительность их соединений;

– количество и размеры переданных пакетов.

После сбора данных их необходимо подготовить для использования в обучении модели, для этого выполняются следующие действия:

– очистка ненужных данных, таковыми являются дубликаты, ошибки или пустые значения в тексте;

– нормализация числовых значений с помощью минимаксной нормализации или z-стандартизация;

– преобразование текстовых значений в числовые представления;

– разделение данных на обучающую, валидационную и тестовую выборки (обычно в соотношении 70/15/15), как представлено на рисунке 2.

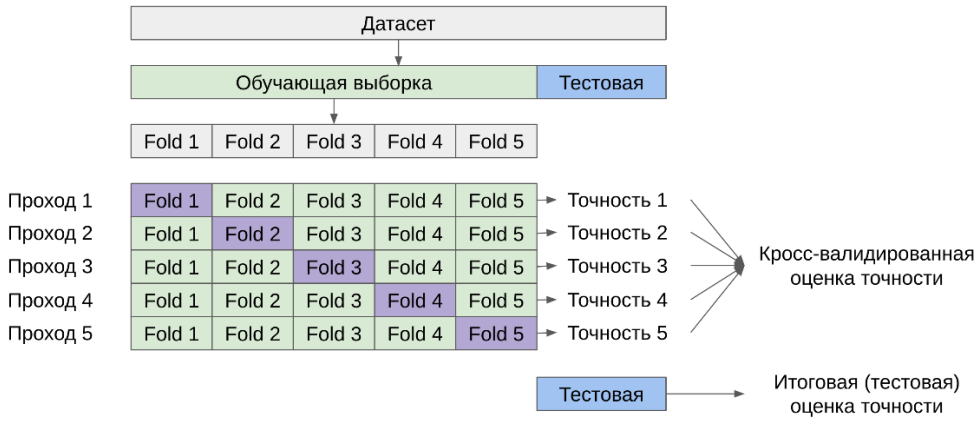

Рисунок 2 – Разделение набора данных на выборки

Созданный набор данных уже можно использовать для обучения нейросети. Однако данная модель способна только определять тип атаки и факты совершенного вторжения. В данной ситуации применение метода Байеса позволяет модели на основе наблюдений предсказывать проведения и типы атак в виде процентной вероятности по их первичным значениям.

Набор, представленный в таблице 2, для задачи обнаружения вторжений в сети передачи данных с применением метода Байеса не отличается по своей структуре от обычного набора данных, представленного в таблице 1, используемого для обучения нейросетей. Однако его использование предполагает дополнительный шаг с расчетом

вероятности проведения атаки по формуле 1.

Таблица 1

Набор данных для обучения нейросети

№ п/п	Время	IP-адрес источника	IP-адрес отправителя	Протокол	Размер пакета	Длительность потока, сек.	Метка
1	2023-10-01 12:00	192.168.1.1	192.168.1.2	*TCP*	1500	1.2	*Normal*
2	2023-10-01 12:01	192.168.1.3	192.168.1.4	*UDP*	500	0.5	*Attack*
…	…	…	…	…	…	…	…
n	2023-10-01 12:02	192.168.1.3	192.168.1.3	*TCP*	800	1.1	*Attack*

Таблица 2

Набор данных для обучения нейросети с вероятностью Байеса

№ п/п	Время	IP-адрес источника	IP-адрес отправителя	Протокол	Размер пакета	Длительность потока, сек.	Метка	*P (Normal|X)*	*P (Attack|X)*
1	2023-10-01 12:00	192.168.1.1	192.168.1.2	*TCP*	1500	1.2	*Normal*	0.95	0.05
2	2023-10-01 12:01	192.168.1.3	192.168.1.4	*UDP*	500	0.5	*Attack*	0.10	0.90
…	…	…	…	…	…	…	…	…	…
n	2023-10-01 12:02	192.168.1.3	192.168.1.3	*TCP*	800	1.1	*Attack*	0.15	0.85

Пример вычисления вероятности выглядит следующим образом.

У нас есть набор наблюдаемых данных, по формуле 1 вычисляются вероятности событий и на их основе указывается метка атаки (*Normal* или *Attack*).

После обучения модели проводится её тестирование. Данный этап является ключевым в процессе разработки системы обнаружения вторжений. Оно позволяет оценить, насколько хорошо модель справляется с задачей классификации новых данных, и выявить ее слабые места. Основными метриками для оценки модели являются:

– точность (*Accuracy*), то есть доля правильно классифицированных примеров;

– полнота (*Recall*): доля правильно обнаруженных аномалий;

– *F*1-мера: гармоническое среднее между точностью и полнотой.

На основе проведенного тестирования принимается решение по поводу введении модели в работу информационно-вычислительной сети:

– модель показывает высокую точность и полноту – готова к использовани;

– модель плохо обнаруживает атаки – требуется дополнительное обучение или сбор новых данных;

– модель часто ошибается на нормальных событиях – пересмотреть порог принятия решений.

Создание базы данных для обучения нейросети, предсказывающей вторжения на основе метода Байеса, это сложный, но крайне важный процесс, открывающий новые возможности для анализа сетевого трафика и выявления сложных атак. Использование данного метода позволяет улучшить точность модели, адаптироваться к новым угрозам и принимать более обоснованные решения. Грамотный подход к сбору, предобработке и аннотации данных позволяет построить надёжную систему обнаружения аномалий, которая поможет защитить информационные системы от киберугроз.

Библиографический список

1. Задбоев, В. А. Исследование уязвимостей алгоритма определения местоположения злоумышленника с помощью средств моделирования процессов / В. А. Задбоев, В. А. Липатников // XXVI Туполевские чтения (школа молодых ученых): Материалы Международной молодёжной научной конференции. Сборник докладов, Казань, 09–10 ноября 2023 года. – Казань: ИП Сагиев А.Р., 2023. – С. 2308-2312. – EDN CNDWQD.

2. Садовников, В. Е. Использование генеративно-состязательных нейросетей для обнаружения и противодействия ботнетам в информационно-коммуникационных сетях / В. Е. Садовников, И. Б. Саенко // Актуальные проблемы инфотелекоммуникаций в науке и образовании : Сборник научных статей XIII Международной научно-технической и научно-методической конференции в 4 т., Санкт-Петербург, 27–28 февраля 2024 года. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2024. – С. 614-618. – EDN JQUJVC.

3. Задбоев, В. А. Алгоритм сканирования сетевой инфраструктуры для выявления внешних злоумышленников / В. А. Задбоев, В. А. Липатников // Инновационные достижения и результаты научной деятельности операторов научных рот Вооруженных Сил Российской Федерации: сборник научных статей по материалам круглого стола, Санкт-Петербург, 29 ноября 2022 года / Военная академия связи. – Санкт-Петербург: ФГКВОУ ВО «Военная академия связи имени Маршала Советского Союза С. М. Буденного» МО РФ, 2022. – С. 89-96. – EDN KQNXRV.

Электронное научное издание

Сборник научных трудов по материалам Международной научно-практической конференции «Современные тенденции в науке, искусстве и технологии: междисциплинарные перспективы»

10 апреля 2025г.

По вопросам и замечаниям к изданию, а также предложениям к сотрудничеству обращаться по электронной почте mail@scipro.ru

Подготовлено с авторских оригиналов

Формат 60x84/16. Усл. печ. Л 0,8. Тираж 100 экз.
Lulu Press, Inc. 627 Davis Drive Suite 300
Morrisville, NC 27560
Издательство НОО Профессиональная наука
Нижний Новгород, ул. М. Горького, 4/2, 4 этаж, офис №1