УДК 004.056.5

АНАЛИЗ УГРОЗ БЕЗОПАСНОСТИ В СЕТЯХ 6G С ПРИМЕНЕНИЕМ МОДЕЛЕЙ МАШИННОГО ОБУЧЕНИЯ

Лоскутова В.С.
специалист, Кубанский государственный университет (Краснодар, Россия)

SECURITY THREAT ANALYSIS IN 6G NETWORKS USING MACHINE LEARNING MODELS

Loskutova V.S.
specialist degree, Kuban state university (Krasnodar, Russia)

Аннотация

В статье рассматриваются актуальные угрозы безопасности, возникающие в сетях шестого поколения (6G), и анализируется потенциал применения моделей машинного обучения (МО) для их обнаружения и предотвращения. Представлена классификация типовых атак, выявлены соответствующие методы МО, обоснована необходимость дифференцированного подхода к выбору алгоритмов. Особое внимание уделено вопросам архитектуры интеграции аналитических моделей в распределённую инфраструктуру 6G, а также оценке их эффективности по ряду технических и эксплуатационных метрик. Сделан вывод о необходимости построения адаптивных, объяснимых и энергоэффективных систем безопасности с возможностью масштабирования и локального анализа.

Ключевые слова: сети 6G, безопасность, машинное обучение, обнаружение угроз, аномалия, интерпретируемость, распределённая архитектура.

Abstract

The article explores emerging security threats in sixth-generation (6G) networks and evaluates the applicability of machine learning (ML) models for threat detection and prevention. It provides a typology of common attack vectors, matches them with relevant ML techniques, and emphasizes the importance of selecting context-specific algorithms. The paper further discusses architectural considerations for integrating ML into the distributed infrastructure of 6G and presents a comprehensive evaluation framework based on technical and operational metrics. The study concludes that adaptive, interpretable, and energy-efficient security systems are essential for maintaining resilience and enabling localized analysis in next-generation networks.

Keywords: 6G networks, security, machine learning, threat detection, anomaly, interpretability, distributed architecture.

Введение

С переходом от пятого поколения мобильной связи к шестому значительно расширяются функциональные возможности беспроводных сетей, включая ультранизкую задержку, экстремально высокую пропускную способность и интеграцию искусственного интеллекта в архитектуру сети. Однако наряду с этим усиливается сложность её структуры, что порождает новые векторы атак и требует принципиально иного подхода к обеспечению безопасности. Современные традиционные методы реагирования и анализа инцидентов становятся недостаточными в условиях высокой динамичности 6G-среды и усложнения угроз. Особенностью сетей 6G является тесное взаимодействие с распределёнными вычислениями, киберфизическими системами и автономными устройствами. Это создаёт предпосылки для

возникновения мультиуровневых атак, включая манипуляции с управлением доступом, внедрение вредоносных моделей искусственного интеллекта и целевые атаки на архитектурные компоненты. Учитывая необходимость обнаружения таких угроз в реальном времени, особую актуальность приобретает внедрение методов машинного обучения, способных анализировать аномалии, выявлять нетипичное поведение и адаптироваться к новым сценариям угроз. Целью данной работы является исследование эффективности применения моделей МО в задачах анализа и выявления угроз безопасности в сетях 6G. В статье рассматриваются типология атак, характеристики сетевой телеметрии, применимые алгоритмы, а также обсуждаются архитектурные и вычислительные аспекты их внедрения. Анализ проводится с учётом требований к масштабируемости, точности, интерпретируемости и скорости реагирования в условиях будущей инфраструктуры шестого поколения связи.

Основная часть

Сети шестого поколения представляют собой следующую ступень эволюции мобильной связи, в рамках которой реализуются не только экстремальные технические параметры, но и глубокая интеграция с когнитивными вычислениями, распределённым интеллектом и цифровыми двойниками. Однако с расширением архитектурных и функциональных возможностей увеличивается поверхность потенциальных атак, а характер угроз становится всё более динамичным и трудно предсказуемым. Основными целями злоумышленников в подобных средах являются перехват или подделка управляющих сообщений, атаки на целостность сетевого взаимодействия, внедрение фальсифицированных устройств и вмешательство в процессы принятия решений на уровне ИИ-модулей. В условиях масштабируемых, гетерогенных и адаптивных сетей 6G традиционные механизмы обеспечения безопасности - такие как сигнатурный анализ, статическая фильтрация или централизованный контроль доступа - оказываются неэффективными или требуют чрезмерных ресурсов. В отличие от них, методы машинного обучения способны выявлять ранее неизвестные аномалии, прогнозировать вредоносную активность и адаптироваться к новым шаблонам поведения. Наиболее перспективными направлениями применения МО являются обнаружение вторжений, классификация сетевых угроз, сегментация вредоносного трафика и выявление атак на протоколы связи в режиме реального времени [1]. Особое внимание в контексте 6G привлекают распределённые модели МО, способные функционировать на периферийных узлах сети (edge-компонентах), минимизируя задержки и уменьшая нагрузку на центральные вычислительные ресурсы. Использование таких подходов позволяет реализовать детекцию атак на месте их возникновения, не прибегая к передаче больших объёмов чувствительных данных. Кроме того, комбинация различных методов обучения - как с учителем, так и без него - обеспечивает более гибкую реакцию на сложные и быстро изменяющиеся угрозы, характерные для мультиагентных сетей нового поколения.

Одной из ключевых задач при анализе угроз в сетях 6G является обработка и интерпретация высокообъёмных потоков телеметрических данных, включающих параметры трафика, временные метки, сигнальные характеристики, сетевые события и поведенческие шаблоны абонентов. В условиях постоянного роста числа подключённых устройств и высокой скорости передачи данных возникает необходимость в использовании алгоритмов, способных не только работать с неструктурированными и разреженными наборами, но и масштабироваться без потери точности [2]. Алгоритмы МО, такие как случайные леса, градиентный бустинг, сверточные нейронные сети и модели, основанные на рекуррентных связях, демонстрируют высокую эффективность при обработке таких данных, позволяя дифференцировать типы активности и выявлять потенциальные угрозы с учётом временных зависимостей. Наряду с точностью классификации и скоростью обработки важную роль играет интерпретируемость моделей, особенно в критически важных инфраструктурах, где требуется объяснение причин принятия решений. Современные подходы в области объяснимого машинного обучения (XAI) позволяют анализировать вклад отдельных признаков в итоговую оценку угрозы, формировать отчёты для аудиторов и повышать уровень доверия со стороны операторов. В сетях 6G, где решения по безопасности могут приниматься

автономными агентами, возможность трактовать результаты классификации и детекции становится неотъемлемым требованием для сертификации и соответствия нормативным требованиям различных государств.

Особое внимание уделяется использованию методов обучения без учителя для обнаружения ранее неизвестных или нестандартных угроз, характерных для гибридных и мультидоменных атак в сетях 6G. Такие методы, как кластеризация, понижение размерности и вероятностные графовые модели, позволяют строить представление об обычном поведении системы и идентифицировать отклонения, не требуя заранее размеченных наборов данных. Это особенно актуально в условиях ограниченной доступности достоверных выборок и постоянно изменяющегося ландшафта атак [3]. Кроме того, сочетание этих подходов с методами полуобучения и активного обучения позволяет итеративно улучшать качество моделей, постепенно расширяя границы известных угроз. Важной задачей в рамках интеграции МО в инфраструктуру 6G является обеспечение защищённости самих моделей от целевых атак, таких как отравление данных (data poisoning), генерация противостоящих примеров (adversarial examples) и подделка телеметрии. Такие атаки могут приводить к ложным срабатываниям, усыплению системы или даже управляемому игнорированию критически опасной активности. Для противодействия этим рискам исследуются подходы по защите жизненного цикла моделей, включая мониторинг обучающих выборок, внедрение механизмов верификации источников данных, а также регулярную переоценку параметров модели с учётом метрик устойчивости и доверия.

Сравнительный анализ моделей случайный лес и глубокая нейронная сеть по параметрам эффективности

Для оценки применимости различных моделей машинного обучения в задачах обнаружения угроз в сетях 6G проведено сравнение двух алгоритмов: случайный лес и глубокая нейронная сеть [4]. Выбор обусловлен их распространённостью в практике анализа сетевого трафика и способностью работать с высокоразмерными, нерегулярными данными. Модели тестировались на наборе симулированных сетевых событий, отражающих аномальное поведение, включая инъекции трафика, сканирование, подмену сигнала и сбои в протоколах. Оценка проводилась по пяти основным критериям: точность обнаружения угроз, устойчивость к ложноположительным срабатываниям, время отклика (инференс), интерпретируемость результатов и вычислительная нагрузка. Каждый показатель нормирован и визуализирован на диаграмме ниже. Это позволяет комплексно оценить пригодность моделей в условиях высоконагруженной, изменчивой среды сетей шестого поколения.

Рисунок 1 демонстрирует сравнительную эффективность двух подходов по ключевым параметрам, включая точность обнаружения, устойчивость к ложным срабатываниям, интерпретируемость, скорость отклика и вычислительную нагрузку, что позволяет комплексно оценить пригодность моделей для различных сценариев применения в сетях 6G.

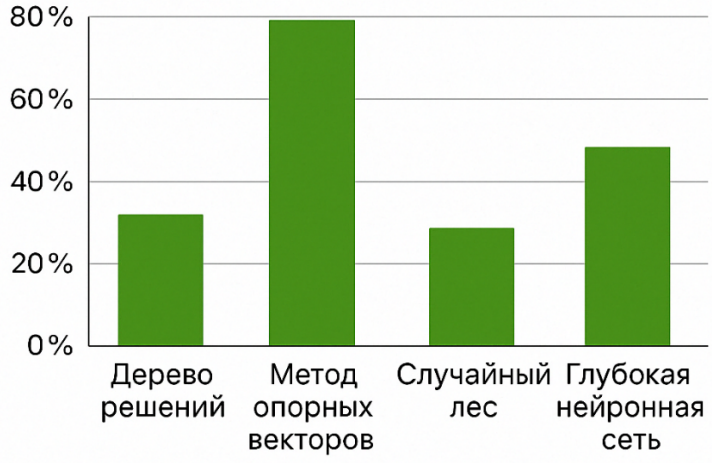

Рисунок 1. Сравнительный анализ моделей случайный лес и глубокая нейронная сеть по эффективности в задачах обнаружения угроз в сетях 6G

Модель случайный лес показала высокую интерпретируемость, устойчивость к ложноположительным срабатываниям и стабильность результатов при умеренной вычислительной нагрузке. Благодаря возможности визуального представления дерева решений и анализа важности признаков, данный алгоритм является предпочтительным для задач, где требуется объяснимость результатов и прозрачность принятия решений, в том числе в регламентированных средах или при необходимости оперативной отчётности перед аудиторами. Кроме того, невысокие требования к ресурсам позволяют внедрять модель на граничных вычислительных узлах с ограниченной производительностью [5].

Глубокая нейронная сеть, напротив, продемонстрировала более высокую точность в обнаружении сложных и неявных аномалий, а также способность адаптироваться к изменяющимся паттернам сетевого трафика. Однако её применение сопряжено с рядом ограничений: значительное время отклика при инференсе, высокая чувствительность к настройке гиперпараметров и затруднённая интерпретация внутренних представлений модели. Эти факторы могут осложнять интеграцию в системы реального времени и требуют дополнительного обеспечения устойчивости к целевым атакам на саму модель.

Таким образом, выбор алгоритма для анализа угроз в сетях 6G должен осуществляться с учётом конкретных условий эксплуатации: критичности к задержкам, доступности вычислительных ресурсов, потребности в объяснимости и типе обрабатываемых угроз. В отдельных сценариях может быть оправдано использование гибридных подходов, объединяющих преимущества обеих моделей.

Сопоставление моделей машинного обучения с типами угроз в сетях 6G

Разнообразие угроз, с которыми сталкиваются сети шестого поколения, требует системного подхода к выбору аналитических инструментов. Учитывая распределённую природу инфраструктуры 6G, высокую динамичность трафика и отсутствие жёстких границ между подсетями, классические универсальные средства реагирования теряют эффективность [6]. В такой среде именно выбор специализированной модели машинного обучения, ориентированной на конкретную категорию угроз, может существенно повысить точность обнаружения, сократить задержку реагирования и снизить уровень ложных срабатываний.

Каждый тип атаки характеризуется определённым набором признаков и векторов воздействия, что обуславливает необходимость дифференцированного подхода к обработке сетевых данных. Некоторые угрозы, такие как инъекция трафика, требуют детального анализа последовательностей пакетов, тогда как для атак на модели обнаружения - важны поведенческие шаблоны и сложные отклонения от нормального функционирования. Кроме того, целесообразность применения конкретного алгоритма зависит от факторов вычислительной нагрузки, интерпретируемости результата, устойчивости к зашумлённым данным и способности адаптироваться к новым сценариям атак [7].

Таблица 1 содержит расширенное сопоставление между типами угроз, их описанием, соответствующими методами машинного обучения, задачами, которые они решают, и преимуществами при их использовании в системах безопасности 6G.

Таблица 1

Расширенное сопоставление угроз и методов машинного обучения в сетях 6G

Тип угрозы	**Характеристика угрозы**	**Применяемый метод МО**	**Цель применения**	**Преимущества подхода**
Инъекция трафика	Изменение или вставка пакетов в поток с целью нарушения логики передачи	Случайный лес	Выявление аномалий на уровне пакетов и сессий	Высокая точность и интерпретируемость при умеренных затратах ресурсов
Сканирование порта	Активный сбор информации об открытых портах и сервисах	Метод опорных векторов	Обнаружение повторяющихся и систематических сканирований	Хорошо работает при малом объёме данных и высокой линейности

Тип угрозы	Характеристика угрозы	Применяемый метод МО	Цель применения	Преимущества подхода
Подделка управляющих сигналов	Фальсификация сигналов управления для манипулирования поведением компонентов сети	Глубокая нейронная сеть	Классификация отклонений в передаче управляющих команд	Глубокое представление сложных зависимостей и паттернов
Атака типа «отказ в обслуживании»	Перегрузка узлов или каналов связи с целью нарушения их доступности	Градиентный бустинг	Быстрое реагирование на нестабильность и высокие нагрузки	Быстрая сходимость и адаптация к изменению трафика
Внедрение вредоносного узла	Имитация легитимных устройств с целью внедрения в доверенные зоны	Кластеризация (без учителя)	Определение нетипичных устройств и поведения в сети	Не требует разметки данных, работает с новыми аномалиями
Атака на модели машинного обучения	Влияние на обучающую выборку или входные данные с целью подрыва надёжности модели	Автоэнкодер + фильтрация аномалий	Защита от атак на алгоритмы обнаружения и классификации	Выявляет скрытые манипуляции и адаптивные обходы моделей

Результаты анализа показывают, что универсального решения не существует: каждая категория угроз требует своего подхода и модели, способной учитывать специфику воздействия. Системы безопасности 6G должны быть гибкими, модульными и опираться на ансамбли алгоритмов, интегрированных в единую аналитическую платформу, способную адаптироваться к меняющейся обстановке и эволюции атакующих стратегий.

Архитектурные особенности интеграции моделей машинного обучения в инфраструктуру 6G

Интеграция методов машинного обучения в инфраструктуру сетей шестого поколения требует учёта специфических особенностей архитектуры 6G, включая высокую плотность распределённых узлов, динамическую маршрутизацию и поддержку вычислений на периферии [8]. В отличие от централизованных решений, применяемых в сетях предыдущих поколений, архитектура 6G предполагает тесную интеграцию средств анализа вблизи источника данных. Это обуславливает необходимость разработки лёгких, ресурсоэффективных моделей, способных функционировать в условиях ограниченной пропускной способности и энергоёмкости.

Одним из ключевых направлений является использование гибридных архитектур, в которых предварительная обработка и первичная фильтрация угроз осуществляются на уровне граничных устройств, а глубокий анализ - в облачной или координирующей части сети. Такой подход обеспечивает баланс между скоростью реагирования и глубиной анализа, позволяя эффективно распределять ресурсы в зависимости от текущей нагрузки [9]. Дополнительно используется подход федеративного обучения, позволяющий обучать модели на локальных данных без их передачи в центральный узел, что повышает конфиденциальность и снижает сетевые издержки.

Не менее важной задачей является обеспечение устойчивости моделей к динамике топологии сети и изменяющимся характеристикам трафика. Для этого применяются адаптивные механизмы, включающие онлайн-обновление весов моделей, использование буферов краткосрочной памяти и переключение между режимами обработки в зависимости от контекста. Такие меры позволяют моделям сохранять релевантность в условиях дрейфа данных и постоянного появления новых типов взаимодействий.

Также важно учитывать аспекты взаимодействия между отдельными интеллектуальными агентами в мультидоменных сетях 6G. В рамках распределённых систем обеспечения безопасности осуществляется координация между локальными детекторами, обмен метаинформацией о выявленных инцидентах и согласование реакций на угрозы. В этой связи актуально применение механизмов коллективного обучения и консенсуса, обеспечивающих сходимость анализа даже при наличии асинхронности и частичной потери информации.

Наконец, важным направлением является обеспечение совместимости внедряемых систем с нормативными требованиями и стандартами будущих телекоммуникационных систем. Реализация гибких политик доступа, логирования и аудита, а также интеграция с платформами доверенного исполнения и защищённой обработки становятся критически важными условиями для успешного применения МО в задачах анализа угроз в сетях 6G.

Метрики оценки эффективности моделей при обнаружении угроз в сетях 6G

Выбор и внедрение моделей машинного обучения для обеспечения сетевой безопасности невозможны без объективной оценки их эффективности. В контексте 6G, где высока нагрузка на каналы связи и критично значение времени реакции, использование стандартных метрик должно дополняться характеристиками, отражающими специфику распределённых систем и вариативность атакующих воздействий. Кроме того, необходимо учитывать не только точность классификации, но и способность модели выявлять редкие и новые типы угроз, а также устойчивость к зашумлённым или искажённым данным.

Классические метрики, такие как точность (accuracy), полнота (recall), специфичность (specificity) и F-мера, по-прежнему остаются основой для оценки качества бинарной или многоклассовой классификации. Однако в условиях сетей 6G особое значение приобретает время отклика модели, измеряемое как средняя задержка между поступлением данных и выдачей результата. Эта характеристика определяет применимость модели в системах реального времени и напрямую влияет на способность предотвращать распространение атаки.

Другим важным параметром является устойчивость модели к концептуальному дрейфу, то есть способность адаптироваться к изменениям в поведении пользователей, новых протоколах или изменяющихся схемах взаимодействия. В этом контексте измеряются показатели деградации производительности с течением времени и скорость восстановления после обновления модели. Дополнительно оценивается интерпретируемость решений, особенно в случае использования глубинных нейросетевых структур [10]. Для этих целей применяются методы SHAP, LIME и визуализация значимости признаков.

Также важно учитывать энергетическую эффективность и вычислительную нагрузку модели. Поскольку в 6G-платформах всё чаще используются периферийные узлы и устройства с ограниченными ресурсами, критично снижать энергопотребление при инференсе и уменьшать потребление памяти. Такие показатели, как FLOPS (число операций с плавающей точкой) и потребление ОЗУ, становятся частью комплексной оценки применимости модели в распределённой среде.

Комплексный подход к оценке, включающий сочетание технических, поведенческих и эксплуатационных метрик, позволяет более точно выбирать и адаптировать алгоритмы под конкретные задачи обнаружения угроз. Это особенно важно в многоуровневых системах безопасности 6G, где эффективность должна обеспечиваться не только за счёт высокой точности, но и за счёт способности модели функционировать в условиях ограничений, неопределённости и атакующих воздействий.

Заключение

Развитие сетей шестого поколения сопровождается не только технологическим прогрессом, но и возрастанием сложности киберугроз, что требует пересмотра подходов к обеспечению безопасности. В данной работе рассмотрены ключевые типы атак, характерные для среды 6G, и обоснована необходимость применения моделей машинного обучения как основы для создания адаптивных, масштабируемых и интеллектуальных систем обнаружения угроз. Проведённый анализ показал, что использование МО позволяет выявлять сложные и скрытые аномалии, адаптироваться к изменяющимся шаблонам трафика, а также обеспечивать

обнаружение атак в реальном времени. В статье представлены подходы к сопоставлению методов МО с конкретными типами угроз, даны рекомендации по архитектуре интеграции аналитических моделей, а также рассмотрены ключевые метрики эффективности, включая точность, устойчивость, интерпретируемость и вычислительную нагрузку.

Эффективное применение МО в сетях 6G требует комплексного подхода, включающего координацию вычислений между центром и периферией, защиту самих моделей от целевых атак, обеспечение совместимости с нормативными требованиями и формирование гибкой системы оценки. Дальнейшие исследования могут быть сосредоточены на разработке защищённых архитектур коллективного обучения, оптимизации энергетических затрат и создании стандартов тестирования алгоритмов в условиях сетей нового поколения.

Список литературы

1. Saeed M.M., Saeed R.A., Abdelhaq M., Alsaqour R., Hasan M.K., Mokhtar R.A. Anomaly detection in 6G networks using machine learning methods // Electronics. 2023. Vol. 12. No. 15. P. 3300.
2. Rahman M.A., Hossain M.S. A deep learning assisted software defined security architecture for 6G wireless networks: IIoT perspective // IEEE Wireless Communications. 2022. Vol. 29. No. 2. P. 52-59.
3. Gkonis P.K., Nomikos N., Trakadas P., Sarakis L., Xylouris G., Masip-Bruin X., Martrat J. Leveraging network data analytics function and machine learning for data collection, resource optimization, security and privacy in 6G networks // IEEE access. 2024. Vol. 12. P. 21320-21336.
4. Suomalainen J., Ahmad I., Shajan A., Savunen T. Cybersecurity for tactical 6G networks: Threats, architecture, and intelligence // Future Generation Computer Systems. 2025. Vol. 162. P. 107500.
5. Sakthi U., Alasmari A., Girija S.P., Senthil P., Qamar S., Hariharasitaraman S. Smart Healthcare Based Cyber Physical System Modeling by Block Chain with Cloud 6G Network and Machine Learning Techniques // Wireless Personal Communications. 2024. P. 1-25.
6. Tan Q. Deep Learning-Driven Network Security Situation Awareness Method in 6G Environment // Internet Technology Letters. 2025. Vol. 8. No. 2. P. e70006.
7. Siriwardhana Y., Porambage P., Liyanage M., Ylianttila M. AI and 6G security: Opportunities and challenges //2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit). IEEE. 2021. P. 616-621.
8. Kaur N., Gupta L. An approach to enhance iot security in 6G networks through explainable ai // arXiv preprint arXiv:2410.05310. 2024.
9. Khalid M., Ali J., Mohsin A.R., Roh B.H., Alenazi M.J. Deep learning techniques for enhanced security and privacy in 6G terrestrial–nonterrestrial network architecture // The Journal of Supercomputing. 2025. Vol. 81. No. 4. P. 631.
10. Sirohi D., Kumar N., Rana P.S., Tanwar S., Iqbal R., Hiji M. Federated learning for 6G-enabled secure communication systems: a comprehensive survey // Artificial Intelligence Review. 2023. Vol. 56. No. 10. P. 11297-11389.