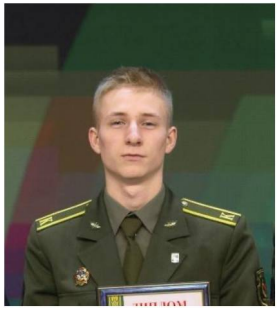
УДК 004.8:004.056

ГРАФОВЫЕ НЕЙРОННЫЕ СЕТИ КАК НАПРАВЛЕНИЕ РАЗВИТИЯ В СИСТЕМАХ БЕЗОПАСНОСТИ СИЛОВЫХ ВЕДОМСТВ

Д.А. Лагутик
Курсант военного факультета БГУИР
lagutikdmitrij40@gmail.com

А.Ю. Савицкий
Старший преподаватель кафедры связи, БГУИР, кандидат военных наук
a.savitskij@bsuir.by



А.Е. Козлов
Курсант военного Факультета БГУИР
anton.kozlov.mailbox@gmail.com

А.Е. Козлов

Обучается в БГУИР по специальности «Компьютерная инженерия». Область научных интересов связана с изучением автоматизации обработки данных с помощью машинного обучения и искусственного интеллекта.

Д.А. Лагутик

Обучается в БГУИР по специальности «Системы и сети инфокоммуникации». Область научных интересов связана с изучением автоматизации обработки данных с помощью машинного обучения и искусственного интеллекта.

А.Ю. Савицкий

Окончил адъюнктуру Военной академии связи имени С.М. Буденного, кандидат военных наук. Область научных интересов связана с совершенствованием научно–методического аппарата оценки эффективности построения систем связи в общевойсковых соединениях и воинских частях, обоснованием принимаемых решений.

Аннотация. Статья раскрывает механизмы интеграции графовых нейронных сетей в системы безопасности силовых ведомств, анализирует действующие случаи внедрения и предлагает архитектурное решение для динамических графов угроз – с поправкой на правовые нормы государств – участников СНГ.

Ключевые слова: Графовые нейронные сети, неевклидовые структуры данных, динамические графы, федеративное обучение, разведывательный анализ, обнаружение аномалий, предиктивная аналитика угроз, масштабируемость данных, защита персональных данных, искусственный интеллект.

Введение. В статье рассматривается потенциал графовых нейронных сетей (Graph Neural Networks, GNN) для задач силовых ведомств, таких как анализ угроз, разведка и кибербезопасность. Предлагается концепция внедрения современных динамических графовых сетей в системы мониторинга и прогнозирования. Рассматриваются преимущества, вызовы и примеры внедрения с опорой на актуальные научные публикации.

Теоретические основы графовых нейронных сетей и основные архитектуры построения. Графовые нейронные сети представляют собой класс моделей глубокого обучения, адаптированных для работы с неевклидовыми структурами данных. В отличие от сверточных сетей, работающих с регулярными сетками, GNN обрабатывают переменное количество узлов и ребер, сохраняя информацию о топологии связей.

Ключевым механизмом GNN является механизм передачи сообщений (message passing): на каждом слое узел агрегирует информацию от соседей, постепенно формируя представления, учитывающие многоуровневые зависимости в графе [1]. Этот процесс имитирует диффузию информации через сеть, где каждый узел обменивается информацией только с непосредственными соседями, но за несколько итераций может уловить глобальную структуру графа, что является основным преимуществом данного подхода. На каждом слое message passing проходит три этапа: каждый соседний узел формирует персонализированное сообщение на основе своих характеристик, данных целевого узла и свойств связи между ними. Затем целевой узел собирает эти сообщения в промежуточное представление, используя простые операции. Наконец, узел обновляет своё состояние, комбинируя предыдущие знания с агрегированной информацией через нейронную сеть, что позволяет постепенно учитывать всё более широкую область графа. Таким образом, для узла v на слое k:

$$h_v^{(k)} = \sigma\left(W^{(k)} \cdot \mathrm{AGGREGATE}^{(k)}\left(\{h_u^{(k-1)} : u \in N(v)\} \right) \right)$$

N(v) – множество соседей узла v, σ – функция активации, $W(k)$ – обучаемые веса, AGGREGATE$^{(k)}$ – функция агрегации сообщений.

Для реализации механизма передачи сообщений данные моделируются в виде графа, где узлы представляют сущности, а ребра – связи между ними (рисунок 1).

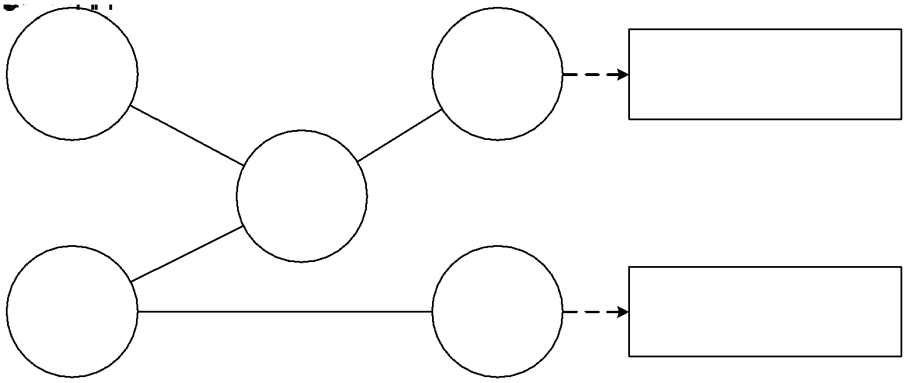


Рисунок 1. Структура графа

h_0, h_1, h_2, h_3, h – узлы гетерогенного графа (графа, элементы которого могут принадлежать к различным типам (категориям), имеющим разную семантику и свойства), [a_1, a_2, a_3 ... a_n] – итоговый вектор–эмбеддинг для узла графа, n – размерность вектора–эмбеддинга (количество признаков), W_{ij} – связь между узлами h_i и h_j.

Основные архитектуры построения графовых нейронных сетей [1]:

1. Graph Convolutional Networks применяют свертку, учитывающую нормировку по степеням узлов, что позволяет сглаживать признаки по локальному окружению. Однако для больших графов вычислительная сложность может стать ограничивающим фактором.

2. GraphSAGE решает проблему масштабируемости за счет сэмплирования фиксированного числа соседей, что делает обучение индуктивным – модель способна генерировать представления для ранее не встречавшихся узлов.

3. Graph Attention Networks вводят механизм внимания, динамически взвешивая вклад каждого соседа при агрегации. Это позволяет модели выделять наиболее значимые связи, что особенно ценно для выявления подозрительных взаимодействий в разведданных.

4. Gated Graph Neural Networks используют рекуррентные архитектуры для обработки динамических графов, где структура связей изменяется во времени.

Однако перечисленные архитектуры изначально ориентированы на статические графы, тогда как реальные сценарии безопасности характеризуются непрерывной эволюцией данных. Для работы с динамическими графами предложены специализированные подходы:

1. EvolveGCN адаптирует параметры во времени с помощью рекуррентных сетей, не требуя знания всех узлов на всем временном интервале, что критично для сценариев с частым изменением состава узлов.

2. Temporal Graph Attention использует функциональное кодирование времени и механизм внимания для агрегации временно–топологических признаков, обеспечивая индуктивное обучение на новых узлах.

3. Temporal Graph Networks представляют универсальную рамку, сочетающую модули памяти и графовые операторы для эффективного обучения на последовательностях временных событий.

Данные подходы позволяют моделировать процессы, где связи и признаки узлов изменяются во времени – например, коммуникационные сети, финансовые транзакции или перемещения объектов [2 – 3].

В силовых ведомствах в сфере анализа данных сводятся к следующему: обнаружение скрытых коммуникаций в условиях намеренной маскировки, выявление аномальных моделей поведения в потоковых данных, прогнозирование перемещений объектов по фрагментарным сигналам, интеграция разнородной информации из несовместимых источников. Традиционные методы машинного обучения упираются в барьер: они теряют топологические зависимости, преобразуя графовые данные в табличные, не способны масштабироваться на сети с миллиардами узлов или не учитывают эволюцию структур во времени. В силовых задачах GNN интегрируют разнородные данные: социальные связи, геолокацию, финансовые потоки. Они превосходят традиционные методы в обнаружении аномалий, поскольку учитывают контекст – изолированный узел с высокой активностью в кластере будет отмечен как угроза, в то время как тот же узел в разреженной сети может оказаться нормой. Преимущества для ведомств: масштабируемость на миллиарды узлов, устойчивость к шуму в данных и способность работать в реальном времени. Например, в системах мониторинга GNN самообучаются на инцидентах, произошедших ранее, минимизируя ложные срабатывания и ускоряя реагирование на новые угрозы [4].

Анализ применения GNN в силовых структурах других стран.

Система MetaConstellation, разработанная Palantir Technologies для Пентагона, представляет собой платформу на базе искусственного интеллекта (ИИ) и графовых моделей для анализа разведданных в реальном времени. Она интегрирует спутниковые снимки, перехваты сигналов, социальные сети и логистику в единый гетерогенный граф. Израильская

система Gospel от Unit 8200 автоматизирует разведку в Газе и Ливане, формируя графы на основе многолетних данных о коммуникациях и перемещениях.Китайская Intelligent Precision Strike System в Силах стратегической поддержки НОАК (Народно-освободительная армия Китая) использует GNN для управления роями дронов и ситуационной осведомленности [5-7].

Несмотря на различия в предметных областях, все три системы демонстрируют общую тенденцию: переход от обработки изолированных данных к моделированию сложных взаимосвязей в динамических графах (таблица 1).

Таблица 1. Сравнительный анализ графовых систем в силовых структурах

Критерии	**MetaConstellation**	**Gospel**	**Intelligent Precision Strike System**
Заказчик	США	Израиль	Китай
Разработчик	Palantir Technologies	Unit 8200	Силы стратегической поддержки НОАК
Тип узлов	Цели, техника, лица	Боевики, телефоны, дома	Дроны, радары, спутники
Тип ребер	Перемещения, коммуникации, транзакции	Звонки, перемещения, покупки	Каналы связи, траектории угроз
Ключевая архитектура	GraphSAGE, GAT	Message passing	Graph Attention
Решаемая задача	Предсказание траекторий угроз, генерация сценариев	Ранжирование целей, трекинг в реальном времени	Управление роем дронов, ситуационная осведомленность
Достигнутый эффект	Сокращение времени анализа с часов до минут (30–50%); точность целеуказания +40%	Сокращение цикла «обнаружение – удар» с дней до часов; эффективность ударов +25–30%	Точность прогноза уязвимостей 85–95%; сокращение времени реакции на 60%; масштабируемость 10000 узлов
Особенность	Explainable AI (визуализация весов внимания)	Контекстный анализ связей для минимизации гражданских потерь	Интеграция киберразведки и помехозащищенность

Рассмотренные системы демонстрируют различные сценарии применения GNN. При этом все они объединяет переход от реактивного анализа (реагирование на уже возникшие события или проблемы на основе исторических данных и текущих сигналов) к предиктивному: вместо фиксации факта коммуникации или перемещения модели предсказывают намерения по цепочкам связей.

Ключевым фактором эффективности выступает способность работать с неполными и зашумленными данными – GNN достраивают недостающие звенья цепочек через топологический контекст, тогда как традиционные методы требуют полной информации.

Кибербезопасность и мониторинг с GNN.

Применение GNN в задачах кибербезопасности демонстрирует устойчивый тренд: переход от изолированного анализа признаков к учету топологических связей обеспечивает качественный рост точности при одновременном снижении ложных срабатываний. Сопоставление результатов независимых исследований 2024 года показывает, что графовые модели систематически превосходят как классические правила, так и нейросетевые базлайны вроде MLP и LSTM (рисунок 2).

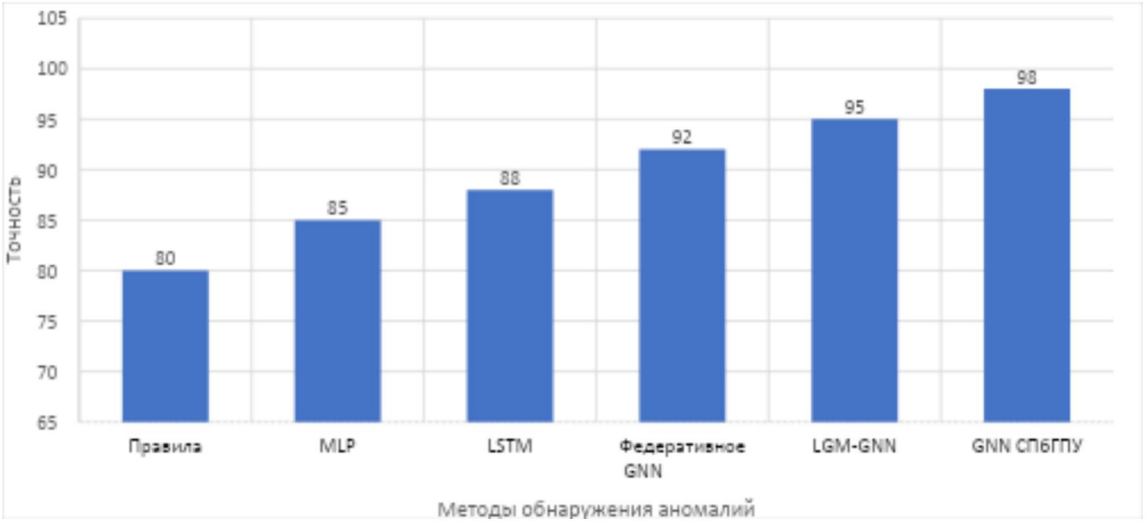


Рисунок 2. Сравнение точности методов обнаружения аномалий

GNN кардинально меняют подход к выявлению аномалий в сетях силовых структур, самообучаясь на помехах и динамических данных, что минимизирует ложные срабатывания по сравнению с традиционными методами. Самообучающиеся GNN мониторят объекты в реальном времени, строя графы трафика (узлы – IP/устройства, ребра – пакеты), где агрегация соседей выявляет скрытые атаки вроде APT (Advanced Persistent Threat) или ботнетов. Министерство внутренних дел Российской Федерации планирует ИИ для поиска правонарушителей, интегрируя GNN в системы видеонаблюдения и соцсетей. Модель на сетевых данных (СПбГПУ, 2024) обнаружила 98% истинных аномалий при FPR всего 2% – в 5–10 раз ниже, чем у MLP или правил. LGM – GNN в финансовых графах достигла accuracy 95%, полноты 92%, снижая FPR на 40%. В спутниковой связи GNN классифицируют трафик с точностью 92–96%, ускоряя анализ в 3 раза. Федеративная GNN для сетевых аномалий показала точность в 92%, сохраняя конфиденциальность данных.

Предлагаемая архитектура для силовых ведомств

Комплексная система на базе GNN строится по трехуровневой схеме, обеспечивающей полный цикл от агрегации разнородных данных до оперативного реагирования и непрерывной адаптации. Каждый уровень решает специфические задачи, критичные для функционирования в условиях высокой динамики угроз и жестких требований к защите информации. (рисунок 3).

Рисунок 3. Предлагаемая комплексная система

Предлагаемая архитектура реализует сквозной конвейер обработки разведывательной информации.

На входном уровне потоковые данные из физически и логически разрозненных источников нормализуются в единое графовое представление с сохранением временных и семантических характеристик.

Ядро системы – гибридный GNN–энкодер, сочетающий индуктивные свойства GraphSAGE (работа с ранее неизвестными объектами без переобучения) и механизмы внимания GAT (динамическое выделение значимых связей и интерпретируемость решений).

Выходной уровень предоставляет программные интерфейсы для взаимодействия с системами реагирования, интерактивную визуализацию для аналитиков и непрерывный мониторинг качества модели с автоматической адаптацией при деградации. Контейнеризированная инфраструктура гарантирует масштабируемость и отказоустойчивость при работе с большими объемами.

Решением проблемы централизации чувствительных данных в GNN является федеративное обучение, которое представляет собой децентрализованный подход к обучению GNN, позволяющий агрегировать знания из распределённых источников данных без их централизации, что особенно актуально для структур государственного уровня.

В контексте графовых сетей модель инициализируется на центральном сервере и рассылается клиентам (ведомствам, региональным узлам), где локально обучается на проприетарных графах трафика или взаимодействий с последующей передачей только градиентов или обновлённых весов.

Важным дополнением к техническим аспектам внедрения искусственного интеллекта является правовое регулирование данной сферы.

В государствах–участниках СНГ с 2021 года ведутся работы по созданию единых подходов к регулированию ИИ в рамках Межгосударственной программы инновационного сотрудничества до 2030 года.

Как отмечается в работе [8], безусловным приоритетом должно стать обеспечение защиты прав человека и его основных свобод перед лицом технологического прогресса. Ключевыми проблемами, требующими законодательного закрепления, остаются вопросы гражданско–правовой и уголовной ответственности за действия автономных систем, поскольку традиционные правовые нормы не всегда применимы к нечеловеческим субъектам.

Кроме того, критическое значение приобретает обеспечение нейтральности и непредвзятости алгоритмов во избежание дискриминационных решений, основанных на смещенных выборках данных.

Особую актуальность в контексте силовых ведомств приобретает принцип транспарентности функционирования технологий ИИ, позволяющий преодолеть эффект «черного ящика» и обеспечить внешний контроль за принимаемыми решениями.

Таким образом, эффективное внедрение интеллектуальных систем невозможно без гармонизированного правового пространства, сочетающего механизмы государственного регулирования и этические принципы, что подтверждается необходимостью разработки специальных нормативных актов, таких как модельный закон для государств–участников СНГ.

Заключение. Графовые нейронные сети переводят анализ угроз силовых ведомств на прогнозирующий уровень, обеспечивая моделирование сложных взаимосвязей в динамических графах. Предложенная архитектура – гибридный GNN–энкодер с федеративным обучением и мониторингом состояния работы – ориентирована на специфику разведывательных задач и требования защиты информации.

Внедрение GNN в силовых структурах крайне важно для поддержания оперативного превосходства: технологии позволяют опережать динамику угроз, минимизировать риски и оптимизировать ресурсы.

Стратегическая потребность во взаимодействии превосходит краткосрочные затраты на настройку инфраструктуры, обеспечивая долгосрочное преимущество в условиях растущей сложности вызовов безопасности. При этом успешное развертывание требует согласования технических решений с правовыми и этическими стандартами, которые формируются в ходе международного сотрудничества.

Список литературы

[1] Mitra S. и др. Use of Graph Neural Networks in Aiding Defensive Cyber Operations / S. Mitra, T. Chakraborty, S. Neupane, A. Piplai, S. Mittal // arXiv. – 2024. – Арх. № 2401.05680v1. – URL: https://arxiv.org/html/2401.05680v1 (дата обращения: 13.03.2026).

[2] Pareja A. и др. EvolveGCN: Evolving Graph Convolutional Networks for Dynamic Graphs / A. Pareja, G. Domeniconi, J. Chen, T. Ma, T. Suzumura, H. Kanezashi, T. Kaler, C. E. Leiserse // IBM Research Publications. – 2020.

[3] Xu, D. Inductive Representation Learning on Temporal Graphs / D. Xu, C. Ruan, E. Körpeoglu, S. Kumar, K. Achan // arXiv preprint. – 2020. – Арх. № 2002.07962. – URL: https://arxiv.org/abs/2002.07962 (дата обращения: 13.03.2026).

[4] Rossi E. и др. Temporal Graph Networks for Deep Learning on Dynamic Graphs / E. Rossi, B. Chamberlain, F. Frasca, D. Eynard, F. Monti, M. M. Bronstein // arXiv. – 2020. – Арх. № 2006.10637. – URL: https://arxiv.org/abs/2006.10637 (дата обращения: 13.03.2026).

[5] Horowitz M.C. Artificial Intelligence, International Competition, and the Balance of Power / M. C. Horowitz // Texas National Security Review.– 2018.– Т. 1, № 3.– С. 36–57.

[6] Аль-Сахель С., Смирнов А. Технологии искусственного интеллекта в палестино-израильском конфликте / С. Аль-Сахель, А. Смирнов // Международная жизнь.– 2023.

[7] Изюмов Д.Б., Кондратюк Е.Л. Анализ различий в подходах США и Китая к применению искусственного интеллекта в системах вооружения / Д. Б. Изюмов, Е. Л. Кондратюк // Инноватика и экспертиза.– 2022.– № 2(34).– С. 228–239.

[8] Абломейко С.В. [и др.] Основные положения модельного закона «Об искусственном интеллекте» / С. В. Абломейко, [и др.] // BIG DATA and Advanced Analytics.– 2024.– Т. 1, №1.– С. 21–31.

Авторский вклад

Козлов Антон Евгеньевич – формализация теоретических основ для разведывательных задач, руководство разработкой рекомендаций по интеграции с национальными платформами безопасности.

Лагутик Дмитрий Александрович – разработка архитектуры GNN, создание методологии поэтапного внедрения графов в командные системы, изучение мировых примеров применения.

Савицкий Алексей Юрьевич – формулировка задачи исследования графовых нейронных сетей в качестве стратегического направления развития систем безопасности силовых структур.

GRAPH NEURAL NETWORKS IN SECURITY SYSTEMS OF LAW ENFORCEMENT AGENCIES

D.A. Lagutik
Student of the military faculty of BSUIR

A.Yu. Savitsky
Senior Lecturer of the Department of Communications, BSUIR, Candidate of Military Sciences

A.E. Kozlov
Student of the military faculty of BSUIR

Abstract. The article examines the mechanisms of integrating graph neural networks into security systems of law enforcement agencies, analyzes existing implementation cases, and proposes an architectural solution for dynamic threat graphs – adjusted to comply with the legal norms of CIS member states.

Keywords: Graph neural networks, non-Euclidean data structures, dynamic graphs, federated learning, intelligence analysis, anomaly detection, predictive threat analytics, data scalability, personal data protection, artificial intelligence.