



**Е.Е. Лунева**

*Томский государственный университет  
систем управления и радиоэлектроники,  
г. Томск, Российская Федерация*

**П.И. Банокин**

*Томский государственный университет  
систем управления и радиоэлектроники,  
г. Томск, Российская Федерация*

## **Графовые нейронные сети в задачах продленной аутентификации групповых профилей социальных сетей**

**Аннотация.** В настоящее время бизнес-процессы многих организаций связаны с необходимостью взаимодействия с групповыми профилями социальных сетей и обработки предоставляемых ими данных. На основе информации из социальных сетей могут проводиться маркетинговые, социологические исследования и различные виды анализа информации, связанные с продуктом, услугами, событиями. Актуальной, в этой связи, становятся методы продленной аутентификации, применяемые в течение пользовательской сессии и позволяющие определить подлинность пользователя на основе поведенческих данных. В данной работе проведен экспериментальный анализ данных, собранных из различных групповых профилей социальной сети, в ходе которого по текстовым данным строится гомогенный граф, каждый узел которого снабжен признаковым описанием, оценивается эффективность метода DOMINANT (Deep Anomaly Detection on Attributed Networks) с использованием графовой нейронной сети для задачи продленной аутентификации.

**Ключевые слова.** Графовая нейронная сеть, продленная аутентификация, социальная сеть, обнаружение аномалий и выбросов, автоэнкодер, ошибка реконструкции.

**Информация о статье.** Дата поступления: 5 июня 2024; дата принятия к публикации: 1 октября 2024 г.; дата онлайн-размещения: 17 октября 2024 г.

Original article

**E.E. Luneva**

*Tomsk State University of Control Systems and Radioelectronics,  
Tomsk, Russian Federation*

**P.I. Banokin**

*Tomsk State University of Control Systems and Radioelectronics,  
Tomsk, Russian Federation*

## **Graph Neural Networks in Tasks of Extended Social Network Group Profiles Authentication**

**Abstract.** Currently, the business processes of many organizations are associated with the need to interact with group profiles of social networks and process the data they

provide. Based on information from social networks, marketing, sociological research and various types of information analysis related to products, services, and events can be carried out. In this regard, methods of extended authentication, used during a user session and allowing to determine the authenticity of the user based on behavioral data, become relevant. In this work, an experimental analysis of data collected from various group profiles of a social network was carried out, during which a homogeneous graph was constructed using text data, each node of which was provided with a feature description, and the effectiveness of the DOMINANT (Deep Anomaly Detection on Attributed Networks) method using graph neural network for the problem of extended authentication.

**Keywords.** Graph neural network, extended authentication, social network, detection of anomalies and outliers, autoencoder, reconstruction error.

**Article info.** Received 5 June, 2024; Accepted 1 October, 2024; Available online 17 October, 2024.

## Введение

Деятельность организаций, предприятий, а также физических лиц сегодня не представляется без использования социальных сетей, которые являются и платформой для общения, и источником информации относительно услуг, продуктов и событий. Профили в социальных сетях, созданные как предприятиями, организациями, так и физическими лицами представляют собой имущественные объекты и могут стать как предметом сделки купли-продажи, так и объектом противоправных действий. В частности, учетная запись администратора профиля, может быть похищена, в результате чего произойдет незаконная смена владельца такого профиля<sup>1</sup>. Таким образом, эффективная деятельность экономических субъектов при взаимодействии с информацией в социальных сетях связана с необходимостью анализировать, оценивать и выявлять изменение в поведении пользователей социальных сетей, которое может быть вызвано изменением редакционной политики или сменой владельца профиля. Актуальным в этой связи становится использование методов продленной аутентификации, выполненной по данным, представленным в профиле социальной сети. Целью настоящей работы является исследование применимости графовых нейронных сетей [1] для решения задачи продленной аутентификации групповых профилей социальных сетей. В рамках настоящего исследования исходными данными для продленной аутентификации являются исключительно тексты публикаций. Источником данных являются сообщества из социальной сети vk.com, а также телеграмм каналы, посвященные экономике, инвестициям и финансам.

<sup>1</sup> Самый читаемый российский Telegram-канал «Бывшая» продали за 1,2 млн р. // РБК. URL: <https://www.rbc.ru/rbcfreenews/59a6fae19a794777c9ac5af7>; «Угонщики» каналов атакуют блогеров // Коммерсантъ. URL: [https://www.kommersant.ru/doc/5772884?from=vertical\\_lenta](https://www.kommersant.ru/doc/5772884?from=vertical_lenta).

### Теоретический обзор

В рамках классического подхода с точки зрения машинного обучения, множество публикаций группового профиля представляет собой множество объектов, каждый объект характеризуется текстом публикации. Таким образом, продленная аутентификация состоит из двух глобальных этапов, обработка текстов и получение численного признакового описания, т.е. каждая публикация заменяется на вектор действительных чисел. Затем на втором этапе к этим данным может быть применен один из методов обнаружения новизны. Обзор методов машинного обучения, применяемых в качестве исходных данных к векторному представлению публикаций группового профиля приведен в работе [2].

Однако, если исходные данные естественным образом образуют некоторую сеть, они могут быть описаны в виде графа, то модель машинного обучения, способная обработать граф, в качестве входных данных, может дать более точные результаты, учитывая, что граф представляет собой совокупность признаков и структурных данных.

Публикации, оставленные в профиле социальной сети характеризуются целым рядом величин, в том числе, время публикации, и использование определенного шаблона повествования, маркерных слов, биграмм, триграмм, использование определенных пунктуационных знаков, принадлежность к определенной теме в рамках набора тем, а также тональность публикации. Опираясь на множество этих данных в качестве исходной модели может быть испробован гетерогенный граф [3], допускающий некоторое заранее заданное множество типов узлов и дуг между ними. Однако, гетерогенный граф значительно сокращает набор методов, который может быть применен для его обработки. И в этой связи, часто используют проекции гетерогенного графа, которые представляют собой гомогенный граф, допускающий один тип узлов и дуг в графе.

Прогнозирование на таких графах может осуществляться на уровне [1]:

1. Узлов, в частности, решать задачу классификации: предсказывать класс узла, 0 нормальная публикация, 1 выброс.

2. Ребер, в частности, предсказывать наличие пропущенного ребра в настоящем и будущем.

3. Графов, в том числе, решать задачу классификации. Если формировать граф по публикациям в некотором временном окне, например, за неделю. То можно прогнозировать нормальный ли это граф или аномальный, относительно всего множества графов, построенных ранее по анализируемому набору публикаций определенного группового профиля социальной сети.

Сам граф, может быть статическим, т.е. выбранная модель машинного обучения может работать только с теми узлами и ре-

брами, которые в момент настройки модели присутствует в графе. Второй тип графа, это динамический, который предполагает, что со временем появляются новые узлы и ребра. В этом случае модель машинного обучения, обеспечивающая обнаружение выбросов/аномалий, может обрабатывать ранее не присутствующие узлы и ребра в графе.

Графовые нейронные сети [1], в отличие от простых энкодеров [3–6], позволяют работать как с признаковым описанием узлов и ребер графа, так и с его структурой. При обработке графов нейронными сетями, происходит трансформация графовой структуры, в частности, узлов графа в векторное представление. Векторное представление узлов графа, формируется опираясь на процедуру передачи сообщения [1], которая заключается в том, что вершины графа посылают *сообщения*, и новое представление каждой вершины получается как некоторая функция  $f$  от: предыдущего представления вершины и агрегированного представления сообщений соседних вершин.

Такая процедура, формирования векторного представления каждой очередной вершины графа, на основе ее предыдущего векторного представления и агрегированного векторного представления соседей называется процедурой графовой свертки. Заключительные слои графовой нейронной сети связаны непосредственно с решаемой задачей классификации или регрессии. В случае отсутствия разметки, сама структура графа используется как «учитель». Например, векторное представление узлов графа, подбирается таким образом, чтобы максимизировать прогноз ребер между узлами графа.

Задача обнаружения аномалий, выбросов, также может быть решена на графах, при помощи графовой нейронной сети. Можно выделить три типа аномалий на графе [7]:

1. Глобальные аномалии, обнаруживаются по атрибутивной составляющей узлов, то есть это узлы, атрибуты которых существенно отличаются от всех остальных узлов графа.

2. Структурные аномалии составляют узлы, имеющие разные модели связей, например, соединение разных сообществ, формирование значительно более плотных связей с другими узлами, по сравнению с общей картиной на графе.

3. Аномалии сообщества позволяют учитывать, как атрибуты узлов, так структуру графа. Вначале граф разбивается на сообщества (группы узлов), далее аномальные узлы определяются как узлы, имеющие разные значения атрибутов по сравнению с другими узлами в рамках одного сообщества.

Анализ существующих в литературе методов обнаружения аномалий на графах позволил выделить нижеописанные методы (табл. 1) [7–14].

Таблица 1

Методы обнаружения аномалий графовыми нейронными сетями

Метод	Тип графа	Мера, по которой оценивается выброс
DOMINANT	Статический, узлы с атрибутами	Оценка аномального поведения
ALARM		Оценка аномального поведения
Fdgars		Вероятность, что узел аномальный
ResGCN		Оценка аномального поведения
OCCGIN	Набор графов	Локация в пространстве признаков описания

Метод DOMINANT (Deep Anomaly Detection on Attributed Networks) [8] не требует разметки, обрабатывает статический граф, каждый узел которого имеет признаковое описание. Данный метод базируется на использовании графовых энкодеров, который включает три части: сверточный энкодер графа позволяет получить векторное представление узлов графа. Далее первый декодер для восстановления структуры графа, который обучается таким образом, чтобы максимально хорошо восстанавливать матрицу смежности графа. Второй декодер, использует векторное представление, сформированное энкодером для восстановления атрибутов узлов графа. Для обучения данной модели используется комплексная ошибка восстановления:

$$L = (1 - \alpha)R_s + \alpha R_A = (1 - \alpha)\|A - \hat{A}\|_F^2 + \alpha\|X - \hat{X}\|_F^2,$$

где,  $\alpha$  — гиперпараметр, который уравнивает результаты структурной реконструкции и реконструкция атрибутов (0.5 по умолчанию),  $R_s$  — ошибка реконструкции, структуры графа (т.е. по матрице смежности),  $R_A$  — ошибка реконструкции атрибутов узлов графа (т.е. признакового описания),  $A$  — матрица смежности,  $X$  — матрица с признаковым описанием узлов графа,  $\|A - \hat{A}\|_F^2$  — норма Фробениуса матриц.

Усовершенствованный метод ALARM [9], разделяет признаковое описание на подгруппы используя несколько энкодеров и декодеров. Например, для пользователей из социальных сетей (такие атрибуты как семейное положение, количество детей, место рождения могут представлять одно подмножество признаков, характеристики контента — количество постов, фотографий и т.п. — другое подмножество признаков).

Метод Fdgars [10] использует нейронную сеть с двумя слоями графовой свертки и требует частичной разметки. Эксперименты проводились с целью идентифицировать пользователей, оставляющих фиктивные отзывы на продукты.

Метод ResGCN [11] использует нейронную сеть с графовыми свертками с механизмами внимания, который заключается в том,

чтобы формировать векторное представление узлов, с учетом взвешенного векторного представления узлов-соседей. Таким образом, каждый смежный узел вносит не равный вклад в векторное представление текущего узла. Веса в сверточных слоях формируются при помощи остаточной нейронной сети, которая принимает на вход признаковое описание узлов графа, и затем формирует остаточную матрицу на выходе, являющееся представлением признакового описания узлов графа. Для обучения такой комплексной нейронной сети, используется общая целевая функция, основанная на двух ошибках реконструкции: структуры и атрибутов как взвешенная комбинация этих ошибок подобно методу DOMINANT [12].

Метод OCGIN [13] позволяет обрабатывать динамические графы. С точки зрения продленной аутентификации, это значит, что только часть публикаций может быть задействовано в обучении модели и далее, графы, построенные на наборах последующих данных, могут быть использованы той же обученной моделью. В основе данного метода лежит GIN сеть (Graph Isomorphism Network) адаптированная под одноклассовую классификацию для обнаружения выбросов на основе глубокого метода опорных векторов [14].

### Планирование эксперимента

В рамках текущего исследования в качестве исходных данных используются данные из социальной сети vk.com, Telegram. В табл. 2 приведен список каналов (их короткие названия в социальной сети) с характеристиками публикаций на момент проведения исследований. Исходные дата-сеты представлены на github по ссылке <sup>2</sup>.

Таблица 2

#### Список каналов (групповых профилей) для формирования датасетов

Канал	Число публикаций	Символов	Слов
investments tinkoff	1713	1009	136
rbc_investments	3989	661	91
economist	932	332	45
full_brokervtb	9462	1177	161
bitkogan	7809	1829	257
cifrprato72	2417	912	111
long_term_investments	1727	1281	176
lemon_tea	1103	1304	185

В данном исследовании вводятся следующие ограничения: используется статический граф неориентированный невзвешенный граф, каждый узел графа имеет признаковое описание. Признаковое

<sup>2</sup> Датасеты по экономической тематике // github.com. URL: <https://github.com/Elena707070/datasets>.



описание формируется опираясь на частоты использования знаков пунктуации, буквенных биграмм и триграмм, частоту использования наиболее популярных в первых 50 % публикаций биграмм и триграмм. Используемый метод для обнаружения аномалий DOMINANT [8], который был выбран так как обеспечивает идентификацию как структурных, так и атрибутивных аномалий, предполагает работу с гомогенным графом и позволяет сделать первичную оценку о применимости графовых нейронных сетей к задаче обнаружения выбросов в рамках продленной аутентификации.

Ниже приведены шаги эксперимента:

1. Получение оригинальных дата-сетов из социальной сети vk, telegram по списку из табл. 2.

2. Формирование «зараженных дата-сетов», по принципу добавления 10 % последних сообщений из похожего профиля. Похожий профиль выбирается исходя из схожести средней длины публикации в символах и словах.

3. Построение графа по  $k$  ближайшим соседям опираясь на евклидово расстояние. Значение  $k$  подбирается как гиперпараметр.

4. Снабжение узлов графа признаковым описанием, опираясь на стилистические и текстовые характеристики текста.

5. Генерация «зараженного» графа (для случая, если дата-сет оригинальный) в соответствии со следующими методами:

– заражение атрибутов узлов графа выполняется в соответствии с работой [15]. Случайно выбирается  $n$  узлов, для каждого узла  $i$  из  $n$  выбирается  $k$  случайных узлов. Из этих  $k$  узлов выбирается самый далекий от  $i$ -ого узла (обозначим его за  $j$ ). Затем происходит замена признакового описания  $i$ -ого узла на признаковое описание  $j$ -ого узла;

– заражение структуры графа выполняется в соответствии с работой [16]. Случайным образом выбирается  $m$  узлов и затем эти узлы соединяются ребрами между собой образуя клику [2], эти узлы являются аномальными, затем таких клик создается  $n$  штук.

Использование метода DOMINANT для идентификации аномальных узлов как для зараженных датасетов, полученных путем добавления сообщений из похожих профилей, так и зараженных графов, полученных в п. 5.

### Экспериментальный анализ

В ходе экспериментального анализа была проанализирована структура получаемых графов, которые отличаются высокой плотностью связей, что характеризуется средней степенью в диапазоне [48–53], а также высоким коэффициентом кластеризации [0,32–0,41]. Выполнен перебор гиперпараметров графовой нейронной сети DOMINANT [8], лучшими оказался для большинства случаев следующий набор параметров: число соседей ( $k$ ) — 30,

число слоев (num\_layers) — 6, эпох (epoch) — 120, число скрытых слоев (hidden\_dim) 32. В табл. 3 представлены результаты экспериментов на датасетах, в которые были добавлены публикации из похожих групповых профилей.

Таблица 3

**Результаты обнаружения аномалий методом DOMINANT**

Оригинальный датасет/публикации-выбросы из похожего датасета	Средняя степень/коэф. кластеризации	AUC_ROC
rbc_investments/cifrprato72.csv	52/0,32	0,77
cifrprato72/rbc_investments	50/0,37	0,66
economist/rbc_investments	52/0,48	0,62
rbc_investments/economist	52/0,32	0,63
Bitkogan/lemonfortea	52/0,41	0,64
lemonfortea/bitkogan	53/0,41	0,63
brokervtb/long_term_investments	49/0,34	0,65
investments_tinkoff/brokervtb	48/0,41	0,73
Brokervtb/investments_tinkoff	50/0,34	0,66
long_term_investments/lemonfortea	48/0,38	0,62
lemonfortea/long_term_investments	53/0,41	0,62

В табл. 4 приведены результаты экспериментов, поставленных на искусственно зараженной структуре и атрибутов графа по оригинальным дата-сетам. Процент зараженных узлов и атрибутов составляет 10 %.

Таблица 4

**Искусственно зараженные графы**

Дата-сет	Средняя степень в графе/коэф. кластеризации	AUC_ROC
rbc_investments	52/0,32	0,88
cifrprato72	50/0,37	0,86
economist	52/0,49	0,81
bitkogan	55/0,28	0,91
lemonfortea	53/0,42	0,84
brokervtb	49/0,34	0,93
long_term_investments	47/0,38	0,83
investments_tinkoff	48/0,41	0,83

Результаты, полученные в ходе экспериментов, показывают, что заданный способ построения графа позволяет выявлять выбросы смеси двух каналов по одинаковым тематикам с характеристикой качества площади под ROC кривой не ниже 0,62. При этом, тематика всех публикаций групповых каналов привязана к



новостным событиям мировой и российской экономики, что усложняет задачу обнаружения выброса. Искусственное заражение структуры и атрибутов графа показывают, более высокие показатели относительно полученных при составлении смеси каналов, что говорит о том, что выразительная способность используемого признакового описания, а также способа построения графа необходимо улучшать, за счет использования других методов трансформации текста в векторное представление, в том числе, таких как maskedML [17], SentenceTransformers [18], а также используя другой способ построения графа, в том числе построение гетерографов и их проекций.

### Заключение

В настоящей работе была исследована применимость метода DOMINANT обнаружения аномалий в данных представляющих собой графовую структуру в рамках задачи продленной аутентификации групповых профилей социальных сетей. Был проведен экспериментальный анализ на дата-сетях из области экономики и финансов, полученных из социальной сети vk, telegram. В ходе экспериментального анализа были искусственно смоделированы выбросы. Первый тип выбросов получен путем добавления в сообщения из одного группового профиля, публикации из похожего на заданный групповой профиль. Второй тип выбросов сгенерирован на графе, полученный по сообщениям по каждому групповому профилю. Площадь под ROC кривой для выбросов первого типа составила не менее 0,62. Выбросы второго типа модель находит более эффективно: площадь под ROC кривой составила более 0,81. Полученные результаты говорят о перспективности использования данной группы методов — графовые нейронные сети для задач продленной аутентификации, однако необходимо продолжать исследование в направлении использования других методов трансформации текста в векторное представление, которые могли бы улучшить выразительную способность используемого признакового описания в том числе, таких как maskedML [17], SentenceTransformers [18].

### Список использованной литературы

1. Hamilton W.L. Graph Representation Learning / W.L. Hamilton. — Springer, 2020. — 159 p.
2. Современное состояние финансов и тренды, определяющие их развитие / М.А. Авдюшина, А.Даваасурэн, Е.В. Агеева [и др.]. — Иркутск : Изд-во БГУ, 2023. — 420 с. — EDN QJAFBU.
3. Harary F. Graph Theory / F. Harary. — Reading, Massachusetts : Addison-Wesley Publishing Company, 1969. — 308 p.
4. Perozzi B. DeepWalk: Online learning of Social Representations / B. Perozzi, R. Al-Rfou, S. Skiena // Proceedings of the 20th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. — New York, 2014. — P. 701–710.


5. Grover A. Scalable Feature Learning for Networks / A. Grover, J. Leskovec // KDD '16: Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. — New York, 2016. — P. 855–864.
6. LINE: Large-scale Information Network Embedding / J. Tang, M. Qu, M. Wang [et al.] // Proceedings of the 24th International Conference on World Wide WebMay. — Geneva, 2015. — P. 1067–1077.
7. A Comprehensive Survey on Graph Anomaly Detection with Deep Learning / X. Ma, J. Wu, S. Xue, J. Yang // IEEE Transactions on Knowledge and Data Engineering. — 2023. — No. 35(12). — P. 12012–12038.
8. Deep Anomaly Detection on Attributed Networks / K. Ding, J. Li, R. Bhanushali, H. Liu // Proc. SIAM Int. Conf. Data Mining. — Philadelphia, PA: Society for Industrial and Applied Mathematics, 2019. — P. 594–602.
9. A Deep Multi-View Framework for Anomaly Detection on Attributed Networks / Z. Peng, M. Luo, J. Li [et al.] // IEEE Trans. Knowl. Data Eng. — 2020. — No. 34(6). — C. 2539–2552.
10. Fdgars: Fraudster Detection via Graph Convolutional Networks in Online App Review System / J. Wang, R. Wen, C. Wu [et al.] // Companion Proceedings of the 2019 World Wide Web Conference. — New York, 2019. — P. 310–316.
11. ResGCN: Attention-Based Deep Residual Modeling for Anomaly Detection on Attributed Networks / Y. Pei, T. Huang, W. Ipenburg, M. Pechenizkiy // Machine Learning. — 2022. — No. 111. — P. 519–541.
12. Deep Anomaly Detection on Attributed Networks / K. Ding, J. Li, R. Bhanushali, H. Liu. — DOI 10.1137/1.9781611975673.67 // Proceedings of the 2019 SIAM International Conference on Data Mining. — Philadelphia, PA, 2019. — P. 594–602.
13. Zhao L. On Using Classification Datasets to Evaluate Graph Outlier Detection: Peculiar Observations and New Insights / L. Zhao, L. Akoglu // Big Data. — 2023. — No. 3. — C. 151–180.
14. Deep One-Class Classification / L. Ruff, R.A. Vandermeulen, N. Görnitz, L. Görnitz // Proceedings of the 35th International Conference on Machine Learning. PMLR, 2018. — P. 4393–4402.
15. Ding K. Interactive Anomaly Detection on Attributed Networks / K. Ding, J. Li, H. Liu // Proceedings of the Twelfth ACM International Conference on Web Search and Data Mining. — New York, 2019. — P. 357–365.
16. Conditional Anomaly Detection / X. Song, M. Wu, C. Jermaine, S. Ranka // IEEE Transactions on Knowledge and Data Engineering. — 2007. — No. 19(5). — C. 631–645.
17. BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding / J. Devlin, M. Chang, K. Lee, K. Toutanova // Proceedings of NAACL-HLT 2019, Minneapolis, Minnesota, June 2, 2019. — Minneapolis, Minnesota, 2019. — P. 4171–4186.
18. Reimers N. Sentence-BERT: Sentence Embeddings using Siamese BERT-Networks / N. Reimers, I. Gurevych // Proceedings of the 2019 Conference on Empirical Methods in Natural Language Processing and the 9th International Joint Conference on Natural Language Processing. — Hong Kong, 2019. — P. 3982–3992.

## References

1. Hamilton W.L. *Graph Representation Learning*. Springer, 2020. 159 p.
2. Avdyushina M.A., Davaasurehn A., Ageeva E.V., Arbatskaya T.G., Bannokin P.I. *The current state of finance and trends that determine its development*. Irkutsk, Baikal State University Publ., 2023. 420 p. EDN: QJAFBU.
3. Harary F. *Graph Theory*. Reading, Massachusetts, Addison-Wesley Publishing Company, 1969. 308 p.
4. Perozzi B., Al-Rfou R., Skiena S. DeepWalk: Online learning of Social Representations. *Proceedings of the 20th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*. New York, 2014, pp. 701–710.

5. Grover A., Leskovec J. Scalable Feature Learning for Networks. *KDD '16: Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*. New York, 2016, pp. 855–864.
6. Tang J., Qu M., Wang M., Zhang M., Yan J., Mei Q. LINE: Large-scale Information Network Embedding. *Proceedings of the 24th International Conference on World Wide WebMay*. Geneva, 2015, pp. 1067–1077.
7. Ma X., Wu J., Xue S. Yang J. A Comprehensive Survey on Graph Anomaly Detection with Deep Learning. *IEEE Transactions on Knowledge and Data Engineering*, 2023, no. 35(12), pp. 12012–12038.
8. Ding K., Li J., Bhanushali R., Liu H. Deep Anomaly Detection on Attributed Networks. *Proc. SIAM Int. Conf. Data Mining*. Philadelphia, PA, Society for Industrial and Applied Mathematics, 2019, pp. 594–602.
9. Peng Z., Luo M., Li J., Xue L., Zheng Q. A Deep Multi-View Framework for Anomaly Detection on Attributed Networks. *IEEE Trans. Knowl. Data Eng.*, 2020, no. 34, pp. 2539–2552.
10. Wang J., Wen R., Wu C., Huang Y., Xion J. Fdgars: Fraudster Detection via Graph Convolutional Networks in Online App Review System. *Companion Proceedings of the 2019 World Wide Web Conference*. New York, 2019, pp. 310–316.
11. Pei Y., Huang T., Ipenburg W., Pechenizkiy M. ResGCN: Attention-Based Deep Residual Modeling for Anomaly Detection on Attributed Networks. *Machine Learning*, 2022, no. 111, pp. 519–541.
12. Ding K., Li J., Bhanushali R., Liu H. Deep Anomaly Detection on Attributed Networks. *Proceedings of the 2019 SIAM International Conference on Data Mining*. Philadelphia, PA, 2019, pp. 594–602. DOI: 10.1137/1.9781611975673.67.
13. Zhao L., Akoglu L. On Using Classification Datasets to Evaluate Graph Outlier Detection: Peculiar Observations and New Insights. *Big Data*, 2023, no. 3, pp. 151–180.
14. Ruff L., Vandermeulen R.A., Görnitz N., Görnitz L. Deep One-Class Classification. *Proceedings of the 35th International Conference on Machine Learning. PMLR*, 2018, pp. 4393–4402.
15. Ding K., Li J., Liu H. Interactive Anomaly Detection on Attributed Networks. *Proceedings of the Twelfth ACM International Conference on Web Search and Data Mining*. New York, 2019, pp. 357–365.
16. Song X., Wu M., Jermaine C., Ranka S. Conditional Anomaly Detection. *IEEE Transactions on Knowledge and Data Engineering*, 2007, no. 19, pp. 631–645.
17. Devlin J., Chang M., Lee K., Toutanova K. BERT: Pre-training of Deep Bi-directional Transformers for Language Understanding. *Proceedings of NAACL-HLT 2019, Minneapolis, Minnesota, June 2, 2019*. Minneapolis, Minnesota, 2019, pp. 4171–4186.
18. Reimers N., Gurevych I. Sentence-BERT: Sentence Embeddings using Siamese BERT-Networks. *Proceedings of the 2019 Conference on Empirical Methods in Natural Language Processing and the 9th International Joint Conference on Natural Language Processing*. Hong Kong, 2019, pp. 3982–3992.


### Информация об авторах

**Лунева Елена Евгеньевна** — кандидат технических наук, доцент, докторант, кафедра комплексной информационной безопасности электронно-вычислительных систем, Томский государственный университет систем управления и радиоэлектроники, г. Томск, Российская Федерация, email: luneva@tusur.ru,  <https://orcid.org/0000-0001-6734-4359>, SPIN-код: 5591-7812, AuthorID РИНЦ: 698883.

**Банокин Павел Иванович** — младший научный сотрудник, Научно-инжиниринговый центр «Интеллектуальные системы доверенного взаимодействия»,

Томский государственный университет систем управления и радиоэлектроники,  
г. Томск, Российская Федерация, email: bpi@fb.tusur.ru.

### Information about the Authors

**Elena E. Luneva** — PhD in Technical Sciences, Associate Professor, Doctoral Degree Applicant, Department of Integrated Information Security of Electronic Computing Systems, Tomsk State University of Control Systems and Radioelectronics, Tomsk, Russian Federation, e-mail: luneva@tusur.ru,  <https://orcid.org/0000-0001-6734-4359>, SPIN-Code: 5591-7812, AuthorID RSCI: 698883.

**Pavel I. Banokin** — Junior Researcher, Scientific and Engineering Center “Intelligent Systems of Trusted Interaction”, Tomsk State University of Control Systems and Radioelectronics, Tomsk, Russian Federation, email: bpi@fb.tusur.ru.

### Вклад авторов

Все авторы сделали эквивалентный вклад в подготовку публикации. Авторы заявляют об отсутствии конфликта интересов.

### Contribution of the Authors

The authors contributed equally to this article. The authors declare no conflicts of interests.

### Для цитирования

Лунева Е.Е. Графовые нейронные сети в задачах продленной аутентификации групповых профилей социальных сетей / Е.Е. Лунева, П.И. Банокин. — DOI 10.17150/2713-1734.2024.6(3).300-311. — EDN LAQQHA // System Analysis & Mathematical Modeling. — 2024. — Т. 6, № 3. — С. 300–311.

### For Citation

Luneva E.E., Banokin P.I. Graph Neural Networks in Tasks of Extended Social Network Group Profiles Authentication. *System Analysis & Mathematical Modeling*, 2024, vol. 6, no. 3, pp. 300–311. (In Russian). EDN: LAQQHA. DOI: 10.17150/2713-1734.2024.6(3).300-311.