УНИВЕРСИТЕТ ИТМО

НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ
июль–август 2021 Том 21 № 4 http://ntv.ifmo.ru/
SCIENTIFIC AND TECHNICAL JOURNAL OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTICS
July–August 2021 Vol. 21 No 4 http://ntv.ifmo.ru/en/
ISSN 2226-1494 (print) ISSN 2500-0373 (online)

НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК УНИВЕРСИТЕТ ИТМО
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ

doi: 10.17586/2226-1494-2021-21-4-562-570
УДК 004.8 004.056.53

Идентификация аккаунтов пользователей при помощи сравнения изображений: подход на основе pHash

Валерий Дмитриевич Олисеенко[1], Максим Викторович Абрамов[2], Александр Львович Тулупьев[3]✉

[1,2,3] Санкт-Петербургский Федеральный исследовательский центр Российской академии наук, Санкт-Петербург, 199178, Российская Федерация
[1,2,3] Санкт-Петербургский государственный университет, Санкт-Петербург, 199034, Российская Федерация

[1] vdo@dscs.pro, https://orcid.org/0000-0002-3479-0085
[2] mva@dscs.pro, https://orcid.org/0000-0002-5476-3025
[3] alt@dscs.pro✉, https://orcid.org/0000-0003-1814-4646

Аннотация

Предмет исследования. Представлен новый подход к идентификации пользователей различных социальных сетей для определения аккаунтов, которые принадлежат одному человеку. Для этой цели использованы изображения, извлекаемые из цифровых следов пользователей. Новизна подхода заключается в том, что для сравнения применяются не только основные изображения профиля пользователя, но и любые элементы графического контента, публикуемые в его аккаунте. **Метод.** Предлагаемый подход заключается в попарном сравнении изображений по принципу «все-со-всеми», публикуемых пользователями в двух аккаунтах из разных социальных сетей для оценки вероятности принадлежности этих аккаунтов одному пользователю. Сравнение обозначенных элементов графического контента производится с использованием известного метода перцептивного хэша pHash. **Основные результаты.** Выполнен вычислительный эксперимент для оценки результатов, полученных с помощью предложенного подхода. По результатам эксперимента величина метрики f1-score достигла 0,886 при трех совпавших изображениях. Показано, что результаты сравнения изображений при помощи pHash могут использоваться для идентификации аккаунтов как самостоятельный подход, так и дополнять другие подходы. Предложенный алгоритм показал, что может быть применен для дополнения существующих методик компаративного анализа аккаунтов. **Практическая значимость.** Автоматизация разработанного подхода обеспечит формирование инструментальной основы использования метода для агрегации и возможности получения большего количества сведений о пользователях и оценки выраженности их личностных особенностей. Полученный результат может быть применен в процессе формирования цифрового двойника пользователя для дальнейшей оценки его особенностей в задачах защиты от социоинженерных атак, таргетированной рекламы, оценки кредитоспособности и других исследований, связанных с социальными сетями и науками социогуманитарного цикла.

Ключевые слова

социальные сети, идентификация пользователя, обработка изображений, pHash, data science, социоинженерные атаки

Благодарности

Работа выполнена в рамках проекта по государственному заданию СПб ФИЦ РАН СПИИРАН № 0073-2019-0003 (формирование подхода); поддержана Санкт-Петербургским государственным университетом, проект № 73555239 (реализации подхода и его апробации); при финансовой поддержке РФФИ, проект № 20-07-00839 (апробация результатов в прототипе комплекса программ).

Ссылка для цитирования: Олисеенко В.Д., Абрамов М.В., Тулупьев А.Л. Идентификация аккаунтов пользователей при помощи сравнения изображений: подход на основе pHash // Научно-технический вестник информационных технологий, механики и оптики. 2021. Т. 21, № 4. С. 562–570. doi: 10.17586/2226-1494-2021-21-4-562-570

© Олисеенко В.Д., Абрамов М.В., Тулупьев А.Л., 2021

Identification of user accounts by image comparison: the pHash-based approach

Valerii D. Oliseenko[1], Maxim V. Abramov[2], Alexander L. Tulupyev[3]✉

[1,2,3] St. Petersburg Federal Research Center of the Russian Academy of Sciences, Saint Petersburg, 199178, Russian Federation

[1,2,3] Saint Petersburg State University, Saint Petersburg, 199034, Russian Federation

[1] vdo@dscs.pro, https://orcid.org/0000-0002-3479-0085

[2] mva@dscs.pro, https://orcid.org/0000-0002-5476-3025

[3] alt@dscs.pro✉, https://orcid.org/0000-0003-1814-4646

Abstract

The study presents a new approach to the identification of various online social networks' users that allows for matching of accounts belonging to the same person. To achieve this goal, images extracted from digital footprints of users are used. The proposed new approach compares not only the main images of a user's profile, but also all the elements of the graphic content published in a user's account. The described approach requires a pairwise comparison of the images published by users in two accounts from different online social networks on the "all-to-all" principle to assess the probability that these accounts belong to the same user. The comparison of the labeled graphical content elements is performed using the well-known perceptual hash method called pHash. A computational experiment was conducted to evaluate the results obtained by using the proposed approach, the f1-score achieved 0.886 for three matched images. It is shown that the results of the pHash image comparison can be used for account identification as a standalone approach as well as to complement other identification approaches. The proposed algorithm can be used to supplement the existing methods for comparative analysis of accounts. Automation of the proposed approach provides a tool for aggregation and makes it possible to obtain more information about users, assessing the depth of their personality features. The results can be applied to forming a digital twin of the user for further description of his (or her) traits in the tasks of protection against social engineering attacks, targeted advertising, assessment of creditworthiness, and other studies related to online social networks and social sciences.

Keywords

online social networks, user identification, image processing, pHash, data science, social engineering attacks

Acknowledgements

This work was carried out within the framework of the project under the state assignment of SPC RAS SPIIRAS No. 0073-2019-0003 (approach formation); supported by Saint Petersburg State University, project No. 73555239 (implementation of the approach and its approbation); with the financial support of the RFBR, project No. 20-07-00839 (approbation of the results in the prototype of the software package).

For citation: Oliseenko V.D., Abramov M.V., Tulupyev A.L. Identification of user accounts by image comparison: the pHash-based approach. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2021, vol. 21, no. 4, pp. 562–570 (in Russian). doi: 10.17586/2226-1494-2021-21-4-562-570

Введение

В исследовании, осуществленном компанией Verizon[1], был определен ежегодный рост объема кибератак в период 2015–2019 гг. на информационные системы. Причем возрастает доля атак, в которых используются методы социальной инженерии. Специалисты компании Positive Technologies обнаружили, что в 63 % случаев атак на пользователей с целью воровства средств с банковских счетов применяются социоинженерные атаки для установки вредоносного программного обеспечения[2]. Высокая популярность методов социальной инженерии среди злоумышленников связана с относительной простотой проведения такого вида атак, так как чаще всего пользователь является самым незащищенным звеном информационной системы[3,4]. Так происходит в том числе потому, что программно-технические атаки изучаются, а средства защиты от программно-технических атак [1–4] развиваются интенсивнее, причем большим числом исследователей, чем область защиты пользователей от социоинженерных атак [5, 6].

Кроме того, программно-технические системы — среда развития программно-технических атак, и такие атаки, с точки зрения исследователя, уже снабжены хорошо развитыми подходами к формализации, инструментарием анализа и моделирования соответствующих систем и процессов. В случае социоинженерных атак поиск подобных подходов и подготовка инструментария все еще находятся в начальной стадии. Социотехническая система как среда реализации социоинженерной атаки оказывается существенно сложнее формализуемой [7], чем программно-техническая

[1] 2020 Verizon Data Breach Investigations Report. 2020 [Электронный ресурс]. URL: https://www.researchgate.net/publication/343239809_2020_Verizon_Data_Breach_Investigations_Report (дата обращения: 10.06.2021).

[2] Ptsecurity — Актуальные киберугрозы: итоги 2019 года. 2020 [Электронный ресурс]. URL: https://www.ptsecurity.com/ruru/research/analytics/cybersecurity-threatscape-2019/ (дата обращения: 12.06.2021).

[3] Мошенники чаще используют социальную инженерию, заявили эксперты. РИА Новости. 2020 [Электронный ресурс]. URL: https://ria.ru/20191125/1561550614.html (дата обращения: 13.06.2021).

[4] Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

система как среда развития программно-технической атаки, из-за включенности в нее человека.

Важный этап обеспечения защищенности пользователей информационных систем — анализ текущего состояния степени устойчивости к социоинженерным атакам. Согласно подходу [8, 9], оценка степени защищенности пользователя информационной системы от социоинженерных атак строится на основе его профиля уязвимостей, который, в свою очередь, ассоциирован с выраженностью различных личностных особенностей [10]. Для построения профиля уязвимостей пользователя необходимо оценить степень выраженности его личностных особенностей. Данная оценка может быть произведена через анализ информации, в том числе с использованием методов data science, полученной из разных источников, среди которых: знания экспертов (результаты психологических тестов, интервьюирование, проективные (в том числе игровые [11]) методики, сведения из отдела кадров); информация из общедоступных источников (публикации в СМИ, социальные сети и т. д.). Важную роль при этом играет количество и качество собранной о пользователе информации. Таким образом, чем больше будет собранной релевантной информации о пользователе, тем, предположительно, легче будет построить оценки выраженности личностных особенностей. Обычно пользователи имеют несколько аккаунтов в разных социальных сетях, и, в зависимости от специфики социальной сети, публикуют в них разный контент. Так, например, в Twitter чаще всего акцент делается на текстовые сообщения, в Instagram — на фотографии, и др. Нахождение аккаунтов одного пользователя в разных социальных сетях позволит агрегировать больше информации о нем, делать выводы о степени ее непротиворечивости. Уже намечаются подходы к решению этой задачи [12–20], но еще не сформировано устоявшегося набора технологий, позволяющего это сделать. Таким образом, в рамках обозначенного широкого поля исследований актуальной видится задача идентификации аккаунтов пользователей в разных социальных сетях с целью выявления среди них принадлежащих одному человеку.

Предлагаемый подход к идентификации аккаунтов

В данной работе представлен новый подход к идентификации аккаунтов пользователя в различных социальных сетях, относящийся к области data science. Этот подход отличается тем, что исходит из предположения в отношении «привычной практики» пользователей, которые зачастую размещают одни и те же изображения в качестве постов, аватаров (главных изображений профилей) в своих аккаунтах на разных платформах социальных сетей. Существуют различные подходы к анализу постов и аватаров пользователей, однако они не всегда применимы и не дают высокую точность на большом количестве разнородных данных. Так, например, для подходов, анализирующих посты [16, 17], может являться важной информация об источнике поста (репост новости, события, объявления и т. д.) или стилистике написания текста (если пост авторский), что сразу же ограничивает применимость данных подходов только в отношении аккаунтов пользователей, которые имеют такие типы постов. Также стоит отметить, что подход сравнения изображений обладает существенным преимуществом над подходами, основанными на сравнении лиц на аватарах [19, 20], его можно применить к аккаунтам пользователей, которые не публикуют фотографии со своим лицом. Помимо этого, подход сравнения изображений может быть применен к закрытым аккаунтам, у которых доступны только изображение аватара и фамилия с именем, что делает его достаточно широко применимым. Для демонстрации практического использования предлагаемого подхода приведены результаты его апробации на собранном наборе данных, состоящем из аккаунтов пользователей различных социальных сетей.

Теоретическая значимость работы заключается в том, что прием сопоставления изображений в компаративном анализе аккаунтов в различных социальных сетях позволит значительно развить существующие подходы к выявлению сходных аккаунтов. Это достигается за счет включения нового атрибута (результата сравнения изображений) в число оцениваемых параметров новых и существующих моделей идентификации пользователей в различных социальных сетях. Практическая значимость заключается в автоматизации предложенного подхода, что обеспечивает формирование инструментальной основы его использования для агрегации в дальнейшем большего количества сведений о пользователях с целью оценки выраженности их личностных особенностей и, опосредованно, уязвимостей в контексте анализа защищенности от социоинженерных атак. Для этого извлекается информация о пользователе из других его аккаунтов в социальных сетях. Полученный результат может быть применен в процессе формирования цифрового двойника пользователя и дальнейшей оценки его особенностей в задачах защиты от социоинженерных атак, таргетированной рекламы, оценки кредитоспособности и других исследований, связанных с социальными сетями и науками социогуманитарного цикла.

Постановка задачи

Пусть имеется множество пар аккаунтов пользователей из разных социальных сетей. В каждом из аккаунтов есть некоторое множество постов, содержащих изображения. Задача заключается в определении критерия, позволяющего через сравнение опубликованных изображений в двух аккаунтах и оценку результатов этого сравнения идентифицировать (классифицировать, выявить) наиболее точно два аккаунта, которые принадлежат одному пользователю. В данной работе изображения в двух аккаунтах сравниваются по схеме «все-со-всеми».

Сравнение изображений осложнено тем, что собранный набор данных не содержит разметки для изображений, т. е. неизвестно какие изображения совпадают, а какие — нет. Для решения поставленной задачи необходимо ответить на следующие вопросы.

— Как определять совпадающие изображения?

— Какое количество изображений должно совпадать? С помощью какой метрики оценить совпадающие количества?
— Есть ли зависимость по времени в эпизодах публикации похожих или совпадающих изображений в разных социальных сетях у одного пользователя?

Ответы на эти вопросы позволят предложить подход, применение которого даст возможность определять аккаунты в различных социальных сетях, в отношении которых с высокой степенью уверенности можно будет утверждать, что они принадлежат одним и тем же пользователям.

Релевантные работы

Задача идентификации аккаунтов пользователя в разных социальных сетях не является новой, уже существуют методы для ее решения в применении к различным социальным сетям. Среди таких работ можно выделить следующие: опирающиеся на социальное окружение пользователя [12, 13], сопоставление атрибутов [14, 15], социальную активность (лайки, комментарии, посты и др.) [16, 17], геолокацию пользователей [18], сравнение лиц на аватарах пользователей [19, 20]. В [21] предложено сравнение аккаунтов на основе целого списка атрибутов (имени, фамилии, страны, пола, фотографий профиля). Необходимо подчеркнуть, что многие из этих методов применяются только к социальным сетям, не являющимся наиболее популярными в русскоязычном сегменте интернета («Foursquare», «Twitter», «Flickr», «Tumblr» и др.)[1]. Данная работа будет опираться, прежде всего, на цифровые следы, извлекаемые из социальных сетей «ВКонтакте» и «Одноклассники», это обуславливается их популярностью и пересечением пользовательской базы, которое по некоторым оценкам составляет около 19 миллионов аккаунтов[2]. Для решения задачи сравнения изображений между собой необходимо выполнить существующий обзор методов.

В настоящий момент существует множество методов для определения одинаковых изображений, однако не все из них подходят для поставленной задачи из-за скорости работы и уровня выделения абстракций на изображении, т. е. способности метода выделять точки, линии, области, структуру на изображении, которые впоследствии будут сравниваться [22]. Когда пользователь публикует в социальных сетях некоторое изображение, он, как правило, подвергает его предварительной графической обработке. Причем обработка может происходить сначала посредством предлагаемого приложением социальной сети инструментария, затем самим приложением при публикации изображения. Такая обработка может в себя включать изменение соотношения сторон, сжатие, появление специфических артефактов, иные изменения, связанные с особенностями хранения изображения. Необходимо учитывать описанную специфику при выборе соответствующих методов обработки, анализа и идентификации изображений.

В процессе поиска выделено несколько методов для идентификации одинаковых изображений, которые можно разделить на следующие классы: методы на основе перцептивного хэша [23–25], дескриптора GIST [26] и методы на основе нейронных сетей («наивное сравнение», one-shot сиамская нейронная сеть)[3]. В итоге выбран метод на основе перцептивного хэша под названием pHash [24], так как он удовлетворяет сформулированным условиям и позволяет пренебрегать нижними уровнями абстракции изображения (точками, линиями, областями). Также метод может оценить полную структуру изображения, которая не изменяется под воздействием описанных манипуляций. Перцептивные хэши предлагались к использованию в схожей задаче [21], и их различные вариации хорошо зарекомендовали себя. Так, например, в работе [27] перцептивный хэш использован для обнаружения подделок изображений, а в [28] — в качестве основы для распознавания лиц. Цель настоящей работы – расширение существующего инструментария для идентификации аккаунтов пользователей в разных социальных сетях, принадлежащих одному человеку, через разработку алгоритма, который на одном из шагов использует метод сравнения изображений перцептивного хэша (pHash).

Перцептивный хэш (pHash)

Любое изображение можно представить в виде табличной функции:

$$(f(i,j))_{i,j=0}^{\substack{i=n-1\\ j=m-1}} = \begin{pmatrix} (r,g,b)_{0,0} & (r,g,b)_{0,1} & \dots & (r,g,b)_{0,n-1} \\ (r,g,b)_{1,0} & (r,g,b)_{1,1} & \dots & (r,g,b)_{1,n-1} \\ \dots & \dots & \dots & \dots \\ (r,g,b)_{m-1,0} & (r,g,b)_{m-1,1} & \dots & (r,g,b)_{m-1,n-1} \end{pmatrix}, \quad (1)$$

где $i \in [0; n-1]$, $j \in [0; m-1]$ — пространственные координаты пиксела изображения (индексы функции); значения функции — три трехзначных числа, которые определяют интенсивность (0 — минимальная, 255 — максимальная интенсивность) для каждого из цветовых каналов (r — красного, g — зеленого, b — синего). Чем выше сумма значений цветовых каналов, тем светлее пиксел и наоборот. По изменению интенсивности цветовых каналов от пиксела к пикселу возможно построить функцию для каждого цвета, разложив которую при помощи, например преобразования Фурье, выделить высокие и низкие частоты в изображении из (1) [29]. Высокие частоты отражают детализацию (цвет, яркость, насыщенность и др.) изображения, а низкие — его структуру. PHash использует дискретное косинусное преобразование, которое тесно связано с

[1] Статистика социальных сетей в России на 2018 год [Электронный ресурс]. URL: https://hiconversion.ru/blog/statistika-socialnyh-setej-vrossii-na-2018-god/ (дата обращения: 13.06.2021).

[2] Там же.

[3] Поиск похожего изображения [Электронный ресурс]. URL: https://medium.com/@senior_sigan/similar-images-search-ce433491059b#3344 (дата обращения: 13.06.2021).

дискретным преобразованием Фурье [29], что позволяет выделить структуру изображения без учета его детализации:

$$F(i,j) = \sum_{k=0}^{m-1}\sum_{l=0}^{n-1} f(i,j)\cos\left[i\left(k+\frac{1}{2}\right)\frac{\pi}{m}\right]\cos\left[j\left(l+\frac{1}{2}\right)\frac{\pi}{n}\right],$$

где $F(i, j)$ — дискретное косинусное преобразование для матрицы $(f(i,j))_{i,j=0}^{i=n-1\ j=m-1}$.

Изображения с измененным размером, соотношением сторон и цветовыми характеристиками (яркость, контраст, наличие цветовых артефактов и др.) будут иметь одинаковые хэши.

Пример полного цикла преобразования pHash представлен на рис. 1. Применив алгоритм pHash к исходному изображению (рис. 1, *a*), получим хэш вида «0x72a113cb», который можно побитово сравнить с другими хэшами, например, при помощи расстояния Хэмминга [30] для определения одинаковых изображений.

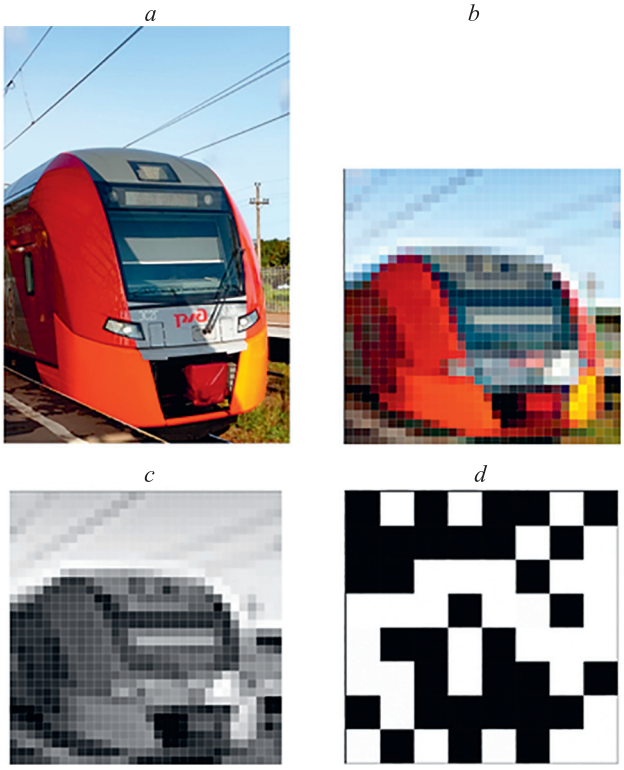

Рис. 1. Пример реализации pHash: исходное изображение (*a*); уменьшенное изображение (32 × 32) (*b*); удаление цвета (*c*); получение графического представления pHash (*d*)

Fig. 1. An example of pHash implementation: original image (*a*); resized image (32 × 32) (*b*); color removal (*c*); obtaining a graphical representation of the pHash (*d*)

Формирование и описание набора данных, метрики

Для выполнения вычислительного эксперимента использован набор данных, впервые представленный в [14], состоящий из 750 открытых аккаунтов пользователей социальных сетей «ВКонтакте» (500 аккаунтов) и «Одноклассники» (250 аккаунтов). Из них сформировано множество пар следующим образом: 50 % пар содержат аккаунты, принадлежащие одному пользователю, остальные 50 % — разным пользователям. Итоговый набор данных включает в себя набор из 500 пар. Для каждого аккаунта были получены все изображения из его альбомов, общее число изображений — 172 251.

Согласно поставленной задаче — определение аккаунтов, принадлежащих одному пользователю – происходит сравнение каждого изображения из одного профиля пары с каждым изображением другого профиля пары. Так как набор данных содержит неразмеченные изображения (т. е. неизвестно какие изображения из двух профилей совпадают, а какие нет), точно оценить совпадение их не представляется возможным, поэтому хэши сравниваются на полное совпадение (расстояние Хэмминга равно 0). Для оценки качества идентификации использованы такие метрики, как precision, recall и f1-score [31]. Данные метрики в работе имеют следующую математическую интерпретацию: пусть tr — порог числа совпадающих изображений, при котором аккаунты считаются принадлежащими одному человеку; TP, FP — число пар, правильно и ошибочно отнесенных к классу аккаунтов, принадлежащих одному человеку; FN — число пар, ошибочно отнесенных к классу аккаунтов, не принадлежащих одному человеку. Тогда precision, recall и f1-score [31] будут иметь следующий вид:

$$\text{precision} = \frac{\text{TP}}{\text{TP} + \text{FP}},$$

$$\text{recall} = \frac{\text{TP}}{\text{TP} + \text{FN}},$$

$$\text{f1-score} = 2\frac{\text{precision}\cdot\text{recall}}{\text{precision} + \text{recall}}.$$

Используя выбранные метрики, определим оптимальный порог tr для идентификации аккаунтов пользователя в разных социальных сетях.

Вычислительный эксперимент

Список средств и библиотек, применяемых при разработке:

— язык Python 3.9;
— среда разработки Jupyter Notebook;
— библиотека Pandas 1.1.14 и NumPy 1.19 — анализ данных;
— библиотека ImageHash — подсчет pHash;
— библиотека request — получение данных из социальных сетей;
— библиотека Matplot 3.3.2 — создание графиков.

Для подсчета хэш-функции pHash использована программная реализация из библиотеки ImageHash (https://pypi.org/project/ImageHash/). В основе данной реализации лежит библиотека Image из пакета PIL (для преобразования изображения в формат 32×32 пиксела) и функция fftpack из библиотеки SciPy (реализация преобразования Фурье). Приведем пример использования реализации pHash из библиотеки ImageHash.

Листинг 1. Пример подсчета pHash

```
imgH = []
for i in df[VK_img]:
    path_to_image = '/imgVK/{}.jpg'.format(i)# путь к папке
    j = imagehash.phash(Image.open(path_to_image))# построение pHash
    imgH.append(np.ndarray.flatten(j.hash))# сохранение pHash
```

Для определения пользовательской активности в каждой из социальных сетей, рассмотрим диаграмму размаха количества опубликованных и совпадающих изображений в двух аккаунтах (рис. 2).

Из рис. 2 видно, что пользователи, имеющие аккаунты в «ВКонтакте» и «Одноклассниках», делают посты с изображениями с разной частотой. Пользователи «ВКонтакте» активнее размещают изображения по сравнению с пользователями «Одноклассников» (больше медиана и межквартальный размах). Это обычно связано с тем, что пользователи посещают одну социальную сеть чаще другой, в некоторых случаях разница в частоте посещений очень большая. Отметим, что количество совпадающих изображений имеет медиану 4 (на рис. 2 отмечены как «Совпадающие»), так как в выборке существуют аккаунты с малым количеством изображений и аккаунты, в которых давно не обновляли посты. Как показал дальнейший эксперимент, идентифицирующая способность подхода высока. Это может быть связано с тем, что пользователи редко удаляют старые изображения, и даже если их малое количество, все равно возможно провести сравнение для таких аккаунтов. При анализе выявлено, что у 11,6 % аккаунтов в сформированном наборе данных нет изображений с лицом, но при этом есть другие изображения. Применим подход к аккаунтам, в которых нет изображений с лицом, с целью увеличения охвата аккаунтов для идентификации. Можно сделать вывод, что подход применим к аккаунтам без изображений с лицом и позволяет анализировать аккаунты, которые ранее исключались из рассмотрения.

В таблице рассчитаны метрики precision, recall и f1-score на тестовом наборе данных. Для расчета последовательно устанавливался порог $tr \in \{1, 2, \ldots, 10\}$, если количество совпадающих изображений было больше или равно данному порогу, то пара аккаунтов определялась как принадлежащая одному пользователю. Задача стояла в определении оптимального порога tr, для которого задача идентификации аккаунтов будет решаться в большинстве случаев и с достаточной точностью. Для выбора оптимального порога tr найдем наибольшее значение метрики f1-score.

Наилучшие показатели метрика f1-score на тестовом наборе имеет при пороге tr = 3. Иными словами, при трех совпадающих изображениях из двух разных аккаунтов в социальных сетях получим лучшую модель классификации. Пороги tr = 1 и tr = 2 не подходят, так как при них происходят слишком часто ложные срабатывания (precision меньше, чем у порога tr = 3). Дальнейшие увеличение порога tr ведет к уменьшению метрики recall. Это означает, что классификатор начинает пропускать без рассмотрения пары аккаунтов, которые принадлежат одному человеку по причине отсутствия в таких аккаунтах достаточного количества одинаковых изображений.

Для определения аккаунтов, принадлежащих одному пользователю, можно использовать следующий алгоритм:

1) извлечь изображения из двух аккаунтов;
2) используя хэш-функцию pHash получить для каждого изображения хэш;
3) попарно сравнить все хэши изображений двух аккаунтов;
4) если число совпадающих изображений равно 3 или больше, то аккаунты принадлежат одному человеку.

Эксперимент показал, что важным аспектом является время публикации одинаковых изображений. Так, на рис. 3 представлена диаграмма размаха для промежутка времени между публикацией одних и тех же изображений в разных социальных сетях.

Из рис. 3 видно, что большинство изображений публикуется в промежутке от 1-го до 3-х дней, с медианой

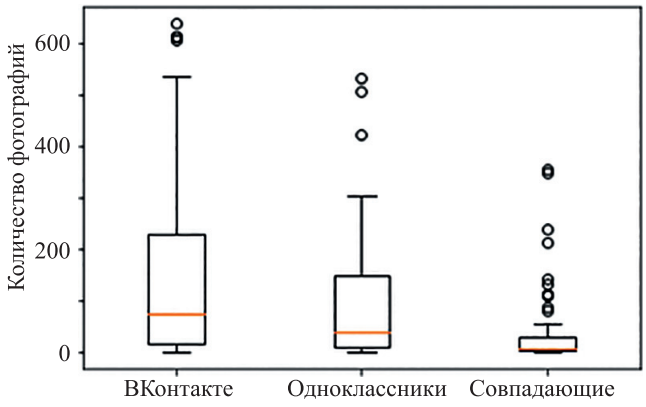

Рис. 2. Пример количества изображений в профилях пользователей

Fig. 2. An example of the number of images in user profiles

Таблица. Расчет метрик

Table. Metrics calculation

tr (порог)	precision	recall	f1-score
1	0,852	0,920	0,885
2	0,886	0,840	0,862
3	0,957	0,825	0,886
4	0,962	0,608	0,745
5	0,962	0,508	0,665
6	0,964	0,473	0,635
7	0,964	0,401	0,566
8	0,971	0,325	0,487
9	0,979	0,317	0,479
10	0,986	0,280	0,436

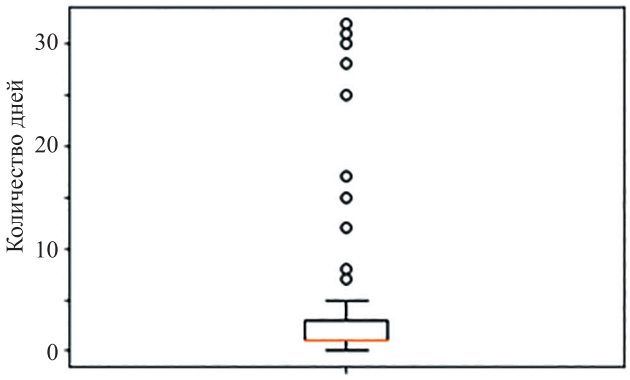

Рис. 3. Время в днях между публикацией одинаковых изображений

Fig. 3. Time (in days) between publishing the same images

в 1 день. Это можно интерпретировать следующим образом – значительная часть людей в выборке стараются обновлять изображения одновременно во всех социальных сетях. Однако оставшаяся часть людей (24,4 %) удалена с рисунка, так как они обновляют изображения не так активно (между обновлениями более 35 дней).

Таким образом, в работе рассмотрен метод сравнения изображений на основе перцептивного хэша pHash и его применение в задаче компаративного анализа аккаунтов пользователей в разных социальных сетях с целью выявления тех, которые принадлежат одному пользователю. По полученным результатам эксперимента можно сделать вывод, что представленный подход способен с высокой точностью идентифицировать профили, как принадлежащие одному пользователю, так и нет, при пороговом значении tr = 3, так как f1-score при данном пороге имеет максимальное значение (0,886). Для определения аккаунтов, принадлежащих одному пользователю, предложен новый алгоритм. Алгоритм не использует какие-либо другие атрибуты, кроме изображений, таким образом его легко адаптировать для социальных сетей, которые акцентированы на публикации графического контента.

Заключение

В работе предложен новый подход к идентификации аккаунтов пользователей из различных социальных сетей для определения тех, которые принадлежат одному человеку. Подход заключается в попарном сравнении изображений по принципу «все-со-всеми», публикуемых пользователями в двух аккаунтах из разных социальных сетей для оценки вероятности принадлежности этих аккаунтов одному пользователю. Новизна подхода заключается в том, что для сравнения используются не только основные изображения профиля пользователя, но и любые элементы графического контента, публикуемые в его аккаунте. Сравнение обозначенных элементов графического контента производится с использованием известного метода перцептивного хэша pHash. Выполнен вычислительный эксперимент для оценки результатов, получаемых с помощью предложенного подхода, по результатам которого величина метрики f1-score достигла 0,886 при трех совпавших изображениях. Теоретическая значимость работы на концептуальном уровне заключается в том, что прием сопоставления изображений в компаративном анализе аккаунтов в различных социальных сетях позволит развить существующие подходы к выявлению среди таких аккаунтов сходных. Результат сравнения изображений при помощи pHash может использоваться для идентификации аккаунтов как самостоятельный подход, так и дополнять другие подходы идентификации, лежащие в области data science. Практическая значимость заключается в автоматизации предложенного подхода, что обеспечивает формирование инструментальной основы его использования для агрегации в дальнейшем большего количества сведений о пользователях с целью оценки выраженности их личностных особенностей и, опосредованно, уязвимостей в контексте анализа защищенности от социоинженерных атак. Дальнейшие направление для исследования нацелено на расширение набора данных, применение представленного подхода для других социальных сетей, которые в большей степени ориентированы на размещение графического контента («Instagram», «Flickr», «TikTok» и др.), и возможное применение для определения фейковых аккаунтов в социальных сетях.

Полученный результат может быть применен в процессе формирования цифрового двойника пользователя и дальнейшей оценки его особенностей в задачах защиты от социоинженерных атак, таргетированной рекламы, оценки кредитоспособности и других исследований, связанных с социальными сетями, науками социогуманитарного цикла.

Литература

1. Mineraud J., Mazhelis O., Su X., Tarkoma S. A gap analysis of Internet-of-Things platforms // Computer Communications. 2016. V. 89-90. P. 5–16. https://doi.org/10.1016/j.comcom.2016.03.015
2. Браницкий А.А., Котенко И.В. Анализ и классификация методов обнаружения сетевых атак // Труды СПИИРАН. 2016. № 2(45). С. 207–244. https://doi.org/10.15622/sp.45.13
3. Parkinson S., Ward P., Wilson K., Miller J. Cyber threats facing autonomous and connected vehicles: Future challenges // IEEE Transactions on Intelligent Transportation Systems. 2017. V. 18. N 11. P. 2898–2915. https://doi.org/10.1109/TITS.2017.2665968
4. Du M., Wang K., Chen Y., Wang X., Sun Y. Big data privacy preserving in multi-access edge computing for heterogeneous Internet of Things // IEEE Communications Magazine. 2018. V. 56. N 8. P. 62–67. https://doi.org/10.1109/MCOM.2018.1701148

References

1. Mineraud J., Mazhelis O., Su X., Tarkoma S. A gap analysis of Internet-of-Things platforms. *Computer Communications*, 2016, vol. 89-90, pp. 5–16. https://doi.org/10.1016/j.comcom.2016.03.015
2. Branitskiy A.A., Kotenko I.V. Analysis and classification of methods for network attack detection. *SPIIRAS Proceedings*, 2016, no. 2(45), pp. 207–244. (in Russian). https://doi.org/10.15622/sp.45.13
3. Parkinson S., Ward P., Wilson K., Miller J. Cyber threats facing autonomous and connected vehicles: Future challenges. *IEEE Transactions on Intelligent Transportation Systems*, 2017, vol. 18, no. 11, pp. 2898–2915. https://doi.org/10.1109/TITS.2017.2665968
4. Du M., Wang K., Chen Y., Wang X., Sun Y. Big data privacy preserving in multi-access edge computing for heterogeneous Internet of Things. *IEEE Communications Magazine*, 2018, vol. 56, no. 8, pp. 62–67. https://doi.org/10.1109/MCOM.2018.1701148

5. Goel S., Williams K., Dincelli E. Got phished? Internet security and human vulnerability // Journal of the Association for Information Systems. 2017. V. 18. N 1. P. 22–44. https://doi.org/10.17705/1jais.00447
6. Абрамов М.В. Автоматизация анализа социальных сетей для оценивания защищённости от социоинженерных атак // Автоматизация процессов управления. 2018. № 1(51). С. 34–40.
7. Khlobystova A., Korepanova A., Maksimov A., Tulupyeva T. An approach to quantification of relationship types between users based on the frequency of combinations of non-numeric evaluations // Advances in Intelligent Systems and Computing. 2020. V. 1156 AISC. P. 206–213. https://doi.org/10.1007/978-3-030-50097-9_21
8. Хлобыстова А.О., Абрамов М.В., Тулупьева Т.В., Тулупьев А.Л. Социальное влияние на пользователя в социальной сети: типы связей в оценке поведенческих рисков, связанных с социоинженерными атаками // Управленческое консультирование. 2019. № 3. С. 104–117. https://doi.org/10.22394/1726-1139-2019-3-104-117
9. Абрамов М.В., Тулупьева Т.В., Тулупьев А.Л. Социоинженерные атаки: социальные сети и оценки защищенности пользователей. СПб.: ГУАП, 2018. 266 с.
10. Азаров А.А., Абрамов М.В., Тулупьева Т.В., Тулупьев А.Л. Анализ защищённости групп пользователей информационной системы от социоинженерных атак: принцип и программная реализация // Компьютерные инструменты в образовании. 2015. № 4. С. 52–60.
11. Krylov B., Abramov M., Khlobystova A. Automated player activity analysis for a serious game about social engineering // Studies in Systems, Decision and Control. 2020. V. 337. P. 587–599. https://doi.org/10.1007/978-3-030-65283-8_48
12. Li Y., Su Z., Yang J., Gao C. Exploiting similarities of user friendship networks across social networks for user identification // Information Sciences. 2020. V. 506. P. 78–98. https://doi.org/10.1016/j.ins.2019.08.022
13. Корепанова А.А., Олисеенко В.Д., Абрамов М.В. Применимость коэффициентов сходства в задаче сравнения социального окружения // Международной конференция по мягким вычислениям и измерениям. 2020. Т. 1. С. 39–42.
14. Корепанова А.А., Олисеенко В.Д., Абрамов М.В., Тулупьев А.Л. Применение методов машинного обучения в задаче идентификации аккаунтов пользователя в двух социальных сетях // Компьютерные инструменты в образовании. 2019. № 3. С. 29–43. https://doi.org/10.32603/2071-2340-2019-3-29-43
15. Raad E., Chbeir R., Dipanda A. User profile matching in social networks // Proc. 13th International Conference on Network-Based Information Systems (NbiS). 2010. P. 297–304. https://doi.org/10.1109/NBiS.2010.35
16. Schwartz H.A., Eichstaedt J.C., Kern M., Dziurzynski L., Ramones S.M., Adrawal M., Shah A., Kosinski M., Stillwell D., Seligman M.E.P., Ungar L.H. Personality, gender, and age in the language of social media: The open-vocabulary approach // PloS One. 2013. V. 8. N 9. P. e73791. https://doi.org/10.1371/journal.pone.0073791
17. Liu S.,Wang S., Zhu F., Zhang J., Krishnan R. HYDRA: Large-scale social identity linkage via heterogeneous behavior modeling // Proc. of the ACM SIGMOD International Conference on Management of Data. 2014. P. 51–62. https://doi.org/10.1145/2588555.2588559
18. Ozga F., Onnela J.-P., DeGruttola V. Bayesian method for inferring the impact of geographical distance on intensity of communication // Scientific Reports. 2020. V. 10. N 1. P. 11775. https://doi.org/10.1038/s41598-020-68583-1
19. Sokhin T., Butakov N., Nasonov D. User profiles matching for different social networks based on faces identification // Lecture Notes in Computer Science. 2019. V. 11734. P. 551–562. https://doi.org/10.1007/978-3-030-29859-3_47
20. Oh S.J., Benenson R., Fritz M., Schiele B. Person recognition in personal photo collections // IEEE Transactions on Pattern Analysis and Machine Intelligence. 2020. V. 42. N 1. P. 203–220. https://doi.org/10.1109/TPAMI.2018.2877588
21. Ranaldi L., Zanzotto F.M. Hiding Your Face Is Not Enough: user identity linkage with image recognition // Social Network Analysis and Mining. 2020. V. 10. N 1. P. 56. https://doi.org/10.1007/s13278-020-00673-4
22. Marr D., Hildreth E. Theory of edge detection // Proceedings of the Royal Society of London. Series B. Biological Sciences. 1980. V. 207. N 1167. P. 187–217. https://doi.org/10.1098/rspb.1980.0020
23. Рудаков И.В., Васютович И.М. Исследование перцептивных хеш-функций изображений // Наука и образование: научное издание МГТУ им. Н.Э. Баумана. 2015. № 8. С. 269–280. https://doi.org/10.7463/0815.0800596

5. Goel S., Williams K., Dincelli E. Got phished? Internet security and human vulnerability. *Journal of the Association for Information Systems*, 2017, vol. 18, no. 1, pp. 22–44. https://doi.org/10.17705/1jais.00447
6. Abramov M.V. Automation of the social networks websites content analysis in the problems of forecasting the protection of the information systems users from social engineering attacks. *Automation of Control Processes*, 2018, no. 1(51), pp. 34–40. (in Russian)
7. Khlobystova A., Korepanova A., Maksimov A., Tulupyeva T. An approach to quantification of relationship types between users based on the frequency of combinations of non-numeric evaluations. *Advances in Intelligent Systems and Computing*, 2020, vol. 1156 AISC, pp. 206–213. https://doi.org/10.1007/978-3-030-50097-9_21
8. Khlobystova A.O., Abramov M.V., Tulupyeva T.V., Tulupyev A.L. Social influence on the user in social network: types of communications in assessment of the behavioral risks connected with the socio-engineering attacks. *Administrative Consulting*, 2019, no. 3, pp. 104–117. (in Russian). https://doi.org/10.22394/1726-1139-2019-3-104-117
9. Abramov M.V., Tulupeva T.V., Tulupev A.L. Social Engineering Attacks: Social Networks and User Security Estimates. St. Petersburg, SUAI Publ., 2018, 266 p. (in Russian)
10. Azarov A.A., Abramov M.V., Tulupyeva T.V., Tulupyev A.L. The analysis of the information systems'' users'' groups protection analysis from the social engineering attacks: the principle and program implementation. *Computer Tools in Education Journal*, 2015, no. 4, pp. 52–60. (in Russian)
11. Krylov B., Abramov M., Khlobystova A. Automated player activity analysis for a serious game about social engineering. *Studies in Systems, Decision and Control*, 2020, vol. 337, pp. 587–599. https://doi.org/10.1007/978-3-030-65283-8_48
12. Li Y., Su Z., Yang J., Gao C. Exploiting similarities of user friendship networks across social networks for user identification. *Information Sciences*, 2020, vol. 506, pp. 78–98. https://doi.org/10.1016/j.ins.2019.08.022
13. Korepanova A.A., Oliseenko V.D., Abramov M.V. Applicability of similarity coefficients in social circle matching. *International Conference on Soft Computing and Measurements*, 2020, vol. 1, pp. 39–42. (in Russian)
14. Korepanova A.A., Oliseenko V.D., Abramov M.V., Tulupyev A.L. Application of machine learning methods in the task of identifying user accounts in two social networks. *Computer Tools in Education Journal*, 2019, no. 3, pp. 29–43. (in Russian). https://doi.org/10.32603/2071-2340-2019-3-29-43
15. Raad E., Chbeir R., Dipanda A. User profile matching in social networks. *Proc. 13th International Conference on Network-Based Information Systems (NbiS)*, 2010, pp. 297–304. https://doi.org/10.1109/NBiS.2010.35
16. Schwartz H.A., Eichstaedt J.C., Kern M., Dziurzynski L., Ramones S.M., Adrawal M., Shah A., Kosinski M., Stillwell D., Seligman M.E.P., Ungar L.H. Personality, gender, and age in the language of social media: The open-vocabulary approach. *PloS One*, 2013, vol. 8, no. 9, pp. e73791. https://doi.org/10.1371/journal.pone.0073791
17. Liu S.,Wang S., Zhu F., Zhang J., Krishnan R. HYDRA: Large-scale social identity linkage via heterogeneous behavior modeling. *Proc. of the ACM SIGMOD International Conference on Management of Data*, 2014, pp. 51–62. https://doi.org/10.1145/2588555.2588559
18. Ozga F., Onnela J.-P., DeGruttola V. Bayesian method for inferring the impact of geographical distance on intensity of communication. *Scientific Reports*, 2020, vol. 10, no. 1, pp. 11775. https://doi.org/10.1038/s41598-020-68583-1
19. Sokhin T., Butakov N., Nasonov D. User profiles matching for different social networks based on faces identification. *Lecture Notes in Computer Science*, 2019, vol. 11734, pp. 551–562. https://doi.org/10.1007/978-3-030-29859-3_47
20. Oh S.J., Benenson R., Fritz M., Schiele B. Person recognition in personal photo collections. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 2020, vol. 42, no. 1, pp. 203–220. https://doi.org/10.1109/TPAMI.2018.2877588
21. Ranaldi L., Zanzotto F.M. Hiding Your Face Is Not Enough: user identity linkage with image recognition. *Social Network Analysis and Mining*, 2020, vol. 10, no. 1, pp. 56. https://doi.org/10.1007/s13278-020-00673-4
22. Marr D., Hildreth E. Theory of edge detection. *Proceedings of the Royal Society of London. Series B. Biological Sciences*,

24. Zauner C. Implementation and benchmarking of perceptual image hash functions: master's thesis. 2010. 94 p.
25. Zauner C., Steinebach M., Hermann E. Rihamark: Perceptual image hash benchmarking // Proceedings of SPIE. 2011. V. 7880. P. 78800X. https://doi.org/10.1117/12.876617
26. Oliva A., Torralba A. Modeling the shape of the scene: a holistic representation of the spatial envelope // International Journal of Computer Vision. 2001. V. 42. N 3. P. 145–175. https://doi.org/10.1023/A:1011139631724
27. Wang X., Zhou X., Zhang Q., Xu B., Xue J. Image alignment based perceptual image hash for content authentication // Signal Processing: Image Communication. 2020. V. 80. P. 115642. https://doi.org/10.1016/j.image.2019.115642
28. Tuncer T., Dogan S., Abdar M., Pławiak P. A novel facial image recognition method based on perceptual hash using quintet triple binary pattern // Multimedia Tools and Applications. 2020. V. 79. N 39-40. P. 29573–29593. https://doi.org/10.1007/s11042-020-09439-8
29. Грузман И.С., Киричук В.С., Косых В.П., Перетягин Г.И., Спектор А.А. Цифровая обработка изображений в информационных системах: учебное пособие. Новосибирск: Изд-во НГТУ, 2002. 352 с.
30. Hamming R.W. Error detecting and error correcting codes // Bell System Technical Journal. 1950. V. 29. N 2. P. 147–160. https://doi.org/10.1002/j.1538-7305.1950.tb00463.x
31. Cook J., Ramadas V. When to consult precision-recall curves // Stata Journal. 2020. V. 20. N 1. P. 131–148. https://doi.org/10.1177/1536867X20909693

1980, vol. 207, no. 1167, pp. 187–217. https://doi.org/10.1098/rspb.1980.0020
23. Rudakov I.V., Vasiutovich I.M. Analysis of perceptual image hash functions. *Science and Education of the Bauman MSTU*, 2015, no. 8, pp. 269–280. (in Russian). https://doi.org/10.7463/0815.0800596
24. Zauner C. *Implementation and benchmarking of perceptual image hash functions*. Master's thesis. 2010, 94 p.
25. Zauner C., Steinebach M., Hermann E. Rihamark: Perceptual image hash benchmarking. *Proceedings of SPIE*, 2011, vol. 7880, pp. 78800X. https://doi.org/10.1117/12.876617
26. Oliva A., Torralba A. Modeling the shape of the scene: a holistic representation of the spatial envelope. *International Journal of Computer Vision*, 2001, vol. 42, no. 3, pp. 145–175. https://doi.org/10.1023/A:1011139631724
27. Wang X., Zhou X., Zhang Q., Xu B., Xue J. Image alignment based perceptual image hash for content authentication. *Signal Processing: Image Communication*, 2020, vol. 80, pp. 115642. https://doi.org/10.1016/j.image.2019.115642
28. Tuncer T., Dogan S., Abdar M., Pławiak P. A novel facial image recognition method based on perceptual hash using quintet triple binary pattern. *Multimedia Tools and Applications*, 2020, vol. 79, no. 39-40, pp. 29573–29593. https://doi.org/10.1007/s11042-020-09439-8
29. Gruzman I.S., Kirichuk V.S., Kosykh V.P., Peretiagin G.I., Spektor A.A. *Digital Image Processing in Information Systems*. Novosibirsk, NSTU Publ., 2002, 352 p. (in Russian)
30. Hamming R.W. Error detecting and error correcting codes. *Bell System Technical Journal*, 1950, vol. 29, no. 2, pp. 147–160. https://doi.org/10.1002/j.1538-7305.1950.tb00463.x
31. Cook J., Ramadas V. When to consult precision-recall curves. *Stata Journal*, 2020, vol. 20, no. 1, pp. 131–148. https://doi.org/10.1177/1536867X20909693

Авторы

Олисеенко Валерий Дмитриевич — младший научный сотрудник, Санкт-Петербургский Федеральный исследовательский центр Российской академии наук, Санкт-Петербург, 199178, Российская Федерация; ассистент, Санкт-Петербургский государственный университет, Санкт-Петербург, 199034, Российская Федерация, SC 57219554703, https://orcid.org/0000-0002-3479-0085, vdo@dscs.pro

Абрамов Максим Викторович — кандидат технических наук, руководитель лаборатории, старший научный сотрудник, Санкт-Петербургский Федеральный исследовательский центр Российской академии наук, Санкт-Петербург, 199178, Российская Федерация; доцент, Санкт-Петербургский государственный университет, Санкт-Петербург, 199034, Российская Федерация, SC 56938320500, https://orcid.org/0000-0002-5476-3025, mva@dscs.pro

Тулупьев Александр Львович — доктор физико-математических наук, профессор, профессор, Санкт-Петербургский государственный университет, Санкт-Петербург, 199034, Российская Федерация; главный научный сотрудник, Санкт-Петербургский Федеральный исследовательский центр Российской академии наук, Санкт-Петербург, 199178, Российская Федерация, SC 13608565400, https://orcid.org/0000-0003-1814-4646, alt@dscs.pro

Authors

Valerii D. Oliseenko — Junior Researcher, St. Petersburg Federal Research Center of the Russian Academy of Sciences, Saint Petersburg, 199178, Russian Federation; Assistant, Saint Petersburg State University, Saint Petersburg, 199034, Russian Federation, SC 57219554703, https://orcid.org/0000-0002-3479-0085, vdo@dscs.pro

Maxim V. Abramov — PhD, Head of Laboratory, Senior Researcher, St. Petersburg Federal Research Center of the Russian Academy of Sciences, Saint Petersburg, 199178, Russian Federation; Associate Professor, Saint Petersburg State University, Saint Petersburg, 199034, Russian Federation, SC 56938320500, https://orcid.org/0000-0002-5476-3025, mva@dscs.pro

Alexander L. Tulupyev — D.Sc., Full Professor, Saint Petersburg State University, Saint Petersburg, 199034, Russian Federation; Head Researcher, St. Petersburg Federal Research Center of the Russian Academy of Sciences, Saint Petersburg, 199178, Russian Federation, SC 13608565400, https://orcid.org/0000-0003-1814-4646, alt@dscs.pro

Статья поступила в редакцию 24.06.2021
Одобрена после рецензирования 06.07.2021
Принята к печати 01.08.2021

Received 24.06.2021
Approved after reviewing 06.07.2021
Accepted 01.08.2021

Работа доступна по лицензии
Creative Commons
«Attribution-NonCommercial»