УДК 004.42 Дата подачи статьи: 28.09.22, после доработки: 25.11.22
DOI: 10.15827/0236-235X.141.097-106 2023. Т. 36. № 1. С. 097–106

Разработка программного инструмента для построения социального графа пользователя социальной сети в задаче анализа его защищенности от многоходовых социоинженерных атак

А.О. Хлобыстова [1], *младший научный сотрудник, aok@dscs.pro*
М.В. Абрамов [1], *к.т.н., руководитель лаборатории, mva@dscs.pro*
В.А. Сазанов [2], *студент, mail@dscs.pro*

[1] *Санкт-Петербургский Федеральный исследовательский центр РАН, лаборатория теоретических и междисциплинарных проблем информатики, г. Санкт-Петербург, 199178, Россия*
[2] *Санкт-Петербургский государственный университет, г. Санкт-Петербург, 199034, Россия*

Проведение данного исследования обусловлено проблемой отсутствия средств визуализации интенсивности взаимодействия пользователей социальной сети «ВКонтакте», а именно отображения метрик, позволяющих оценивать и ранжировать интенсивность взаимодействия как между пользователем и его друзьями, так и друзей друг с другом.

Целью является повышение доступности и оперативности анализа интенсивности взаимодействия между пользователями через автоматизацию визуализации социального графа. При этом предполагается, что числовым коэффициентам дуг социального графа будет сопоставлена оценка интенсивности взаимодействия пользователей на основе данных, извлекаемых из общедоступных источников социальной сети «ВКонтакте».

Для достижения поставленной цели были рассмотрены вопросы оптимизации агрегации необходимых данных, программной реализации функций для построения социального графа, наглядного отображения интенсивности взаимодействия пользователей с возможностью выбора интересующих метрик, создания удобного интерфейса и встраивания разработанного инструментария в веб-приложение.

Предметом исследования являются данные о взаимодействии между пользователями сети «ВКонтакте» и способы их визуализации. Методы работы основаны на оптимизации отправки запросов к интерфейсу API «ВКонтакте», а также на разработке функций и настроек для построения социального графа.

Теоретическая значимость предлагаемого решения заключается в развитии подходов к анализу распространения многоходовых социоинженерных атак и апробированию моделей оценки интенсивности взаимодействия пользователей. Существенная практическая значимость состоит в автоматизации процесса оценки интенсивности взаимодействия сотрудников для принятия эффективных мер по нивелированию рисков успешной реализации социоинженерных атак. Новизна исследования – в улучшении визуализации построения социального графа пользователей «ВКонтакте» через добавление новых метрик для оценки интенсивности взаимодействия пользователей.

Ключевые слова: *социальный граф, социоинженерные атаки, оценка вероятности распространения, визуализация взаимодействия, социальные сети, веб-приложение, информационная безопасность, метрики интенсивности взаимодействия пользователей, архитектура веб-приложения.*

В настоящее время как частные лица, так и различные организации все чаще становятся жертвами социоинженерных атак [1–4]. При этом нередко для достижения целей атаки в нее вовлекается сразу цепочка пользователей, то есть осуществляется многоходовая социоинженерная атака [4, 5]. Между людьми она, как правило, распространяется с разными оценками вероятностей успеха [4, 6, 7]. В качестве источника информации, по которому могут быть построены такого рода оценки, часто выступают социальные сети [4, 8, 9]. При этом инструменты для визуализации оценок распространения многоходовых социоинженерных атак еще не созданы. Они позволили бы нивелировать существующие проблемы в области информационной безопасности [9–11], в частности, лицам, принимающим решения, оперативнее выявлять наиболее уязвимые к атакам места в системе, вводить меры, снижающие ве-

роятность их воздействия [12, 13]. Таким образом, актуальной видится задача разработки инструментов визуализации оценок вероятности распространения многоходовых социоинженерных атак.

Существуют подходы, которые увязывают оценки степени интенсивности взаимодействия между пользователями и оценки вероятности распространения многоходовой социоинженерной атаки [6]. Данное исследование посвящено разработке инструмента для визуализации на социальном графе интенсивности взаимодействия между пользователями. В качестве модели для оценки интенсивности взаимодействия рассматривается модель, предложенная в [14, 15], а источника данных для обозначения параметров модели – социальная сеть «ВКонтакте» как одна из наиболее популярных в России.

Релевантные работы

В результате анализа предметной области на наличие решений со схожей концепцией было найдено пять продуктов, визуализирующих данные о взаимодействии пользователей социальной сети «ВКонтакте». Однако ни один из них не удовлетворяет сразу всем необходимым требованиям, а именно: приложение должно строить социальный граф пользователя, где вершины – это друзья, а ребра – связи с весами на основе метрик, предложенных в [2] (число общих друзей, количество лайков, комментариев, подарков). Кроме того, в доступных сегодня инструментах не реализована возможность построения графа для чужих профилей. Сравнение существующих решений представлено в таблице, а их обзорное описание дано далее.

1. 3D Social Graph – приложение для «ВКонтакте», строящее 3D-модель социального графа с кластеризацией на основе количества общих друзей. Как недостаток можно выделить отсутствие возможности выбора построения на основе других метрик, а также вывода информации о связи между пользователями.

2. VK Messages Visual Statistics – расширение для Google Chrome, визуализирующее отношения между пользователем и его друзьями «ВКонтакте» по количеству сообщений между ними. Так как используются закрытые данные, пользователь может построить граф только для себя исключительно на основе личных сообщений, что не соответствует поставленной цели.

3. Yasiv VK – один из примеров решений для «ВКонтакте», которые на данный момент не поддерживаются. Приложение позволяет строить граф друзей, при нажатии на вершину графа отображать информацию о пользователе, осуществлять поиск по имени и фамилии пользователя, при двойном клике на вершину дополнять граф узлами-друзьями выбранного пользователя.

4. Интерактивный граф друзей – приложение для «ВКонтакте». На момент написания статьи данное решение не функционирует из-за отказа «ВКонтакте» от поддержки Flash-приложений.

5. Прототип веб-приложения sea.dscs.pro [16]. Позволяет автоматизированно извлекать, предобрабатывать, унифицировать и представлять размещаемые пользователями в социальных сетях данные, которые, в свою очередь, дают возможность косвенно оценить их психологические, поведенческие и иные особенности. При помощи этого приложения можно получить анкетные данные о пользователе, размещенные в социальной сети «ВКонтакте», восстановить недостающие атрибуты аккаунтов («возраст» и «город»), получить вероятностную оценку того, что два аккаунта в соци-

Сравнительный анализ аналогов

A comparative analysis of analogues

№	Название	Поддержка в настоящее время	Метрики о взаимодействии пользователей	Отображение чужого социального графа	Число пользователей
1	3D Social Graph	Да	Нет	Да	5 313
2	VK Messages Visual Statistics	Да	Количество сообщений	Нет	Более 10 000
3	Yasiv VK	Нет	Нет	Да	–
4	Интерактивный граф друзей	Нет	Нет	Нет	61 608
5	Веб-приложение sea.dscs.pro	Да	Нет	Нет	–

альных сетях «ВКонтакте» и «Одноклассники» принадлежат одному пользователю, а также построить социальный граф. Однако последний строится без отображения метрик взаимодействия пользователей друг с другом.

Подобные инструменты создаются и востребованы, что подтверждает актуальность разработки. Однако на текущий момент не выявлено решений, подходящих для целей данного исследования.

Постановка задачи

В рамках исследования были поставлены задачи по оптимизации сбора данных о взаимодействии пользователя с его друзьями и их между собой, по разработке функций и настроек для построения социального графа, внедрению графа в веб-приложение, позволяющее пользователю взаимодействовать с социальным графом, построенным на основе выбранных метрик. То есть на вход поступает идентификатор пользователя социальной сети «ВКонтакте», а на выходе требуется получить социальный граф с размеченными дугами, причем разметка дуг визуально должна отличаться для пользователей, более или менее интенсивно между собой взаимодействующих. Интенсивность взаимодействия рассчитывается в соответствии с моделью, предложенной в работе [3].

Построение социального графа

Математическая модель, лежащая в основе визуализации. Согласно [4], оценка вероятности того, что социоинженерная атака распространится между пользователями, с учетом интенсивности различных видов связи будет рассчитываться по формуле $P = 1 - (1 - p_{rel})\times$ $\times(1 - p_{likes})^{count\_likes}(1 - p_{reposts})^{count\_reposts}(1 - p_{com\_photos})^{count\_photos}(1 - p_{com\_groups})^{count\_groups}$, где p_{rel} – вероятность успеха распространения атаки от сотрудника к сотруднику, основанная на типе декларируемой в социальной сети связи; p_{likes}, $p_{reposts}$, p_{com_photos}, p_{com_groups} – оценки вероятностей, характеризующие, соответственно, вклад отдельного эпизода каждого типа связи в оценку вероятности успеха распространения атаки от сотрудника к сотруднику; *count_likes* – сумма лайков пользователей друг другу; *count_reposts* – сумма репостов каждым записей другого; *count_photos* – число совместных фотографий, на которых отмечен другой пользователь; *count_groups* – число групп и публичных страниц, на которые подписаны оба пользователя. После чего в [17] предложенная формула была актуализирована, а именно проведен опрос, моделирующий распространение социоинженерной атаки. Согласно его результатам, значимыми характеристиками интенсивности взаимодействия пользователей стали число общих друзей, подарков, лайков, комментариев. Адаптированная оценка вероятности того, что социоинженерная атака распространится между пользователями, будет следующей: $P = 1 - (1 - p_{com\_friends})^{count\_friends}\times$ $\times(1 - p_{gifts})^{count\_gifts}(1 - p_{likes})^{count\_likes}(1 - p_{reposts})^{count\_reposts}$, где $p_{com\_friends}$, p_{com_gifts}, p_{likes}, $p_{reposts}$ – оценки вероятностей, характеризующие вклад отдельного эпизода каждого типа связи в оценку вероятности успеха распространения атаки от сотрудника к сотруднику; *count_friends* – количество общих друзей пользователей; *count_gifts* – число подарков; *count_likes* – сумма лайков пользователей друг другу; *count_reposts* – сумма репостов каждым записей другого.

Таким образом, в качестве метрик для визуализации были отобраны число общих друзей, подарков, лайков, комментариев.

Методы и технологии. Разработка инструмента для визуализации социального графа велась на основе существующего прототипа веб-приложения sea.dscs.pro, клиент-серверная архитектура которого представлена в [18]. Для реализации прототипа веб-приложения использовался Django – фреймворк для веб-приложений на языке Python. Как основной инструмент для выгрузки необходимой информации из социальной сети выбран Python-модуль для создания скриптов для «ВКонтакте» – vk_api.

Сбор общих друзей пользователя. При построении социального графа важную роль играет информация о взаимосвязях пользователей друг с другом. Вместе с тем отправка неоптимальных запросов к интерфейсу API «ВКонтакте» ведет к медленному построению социального графа и, как следствие, затрудненности оперативного анализа уязвимостей к социоинженерным атакам. Проблема реализации, предложенной в [18], заключалась в использовании неоптимального параметра для нахождения списков общих друзей между исходным пользователем и его друзьями. Для ее решения универсальный метод API «ВКонтакте» execute был заменен на метод vk_api. VkRequestsPool. Для демонстрации разницы между ними рассмотрим пример. Пусть N – количество друзей пользователя, тогда *friends_*

ids[*N*] – список их идентификаторов, *uids_batches*[*M*–1] – разделение списка друзей на подгруппы из *M* пользователей, *friends.getMutual* – метод VK API, который возвращает список идентификаторов общих друзей между парой пользователей. На рисунке 1 изображена схема работы функции в двух различных реализациях. В первом случае максимальное количество пользователей, для которых будут возвращены списки общих друзей, равно 25 (так как выполняется отдельный подзапрос для каждого id), во втором – 2 500 (подзапрос выполняется для списка из 100 id). Это не означает ускорение в 100 раз, но все-таки оптимизирует время получения данных об общих друзьях пользователя. Стоит отметить, что большое количество запросов – это bottleneck системы, работающей с API.

Класс для сбора статистики взаимодействия. В контексте решения поставленной задачи интенсивность взаимодействия пользователей, кроме числа общих друзей, основана на числе подарков, лайков, комментариев. Для сбора этих сведений в прототипе веб-приложения был разработан класс FriendsStatistics, в котором реализованы методы, возвращающие для каждого пользователя информацию о количестве эпизодов его взаимодействия (числе подарков, лайков или комментариев в зависимости от вызванной функции) с друзьями.

Также в классе реализован ряд вспомогательных функций для упрощения работы с основными методами, например, функция для разделения списка id пользователей на части для параллельной отправки запросов к API «ВКонтакте» и функция для сбора информации о публикациях пользователя, которые нужны для дальнейшего сбора статистики по взаимодействию пользователей.

Визуализация графа. Для визуализации графа была выбрана библиотека pyvis, которая позволяет легко и быстро осуществлять графические визуализации и исследовать взаимосвязи данных. Для работы с модулем pyvis был разработан класс SocialGraph, принимающий в качестве параметров информацию о пользователе и его друзьях, собранную с применением методов класса FriendsStatistics, и обрабатывающий поступившие сведения. После этого при помощи методов pyvis и функции get edges from_metrics в граф добавляются вершины и ребра, а также устанавливаются необходимые для визуализации параметры.

Пользовательский интерфейс. При нажатии на кнопки на клиентской части вся необходимая для построения информация уже обработана, поэтому в функцию, отвечающую за отображение графа на странице, передаются уже вычисленные параметры, что уменьшает нагрузку на frontend и делает взаимодействие пользователя с социальным графом удобнее.

По умолчанию граф строится на основе общих друзей, а с помощью кнопок в левом верхнем углу, представленных на рисунке 2, пользователь может выбирать другие параметры для построения графа, такие как подарки, лайки и комментарии.

Под кнопками расположено специальное поле для вывода информации о выбранной вершине или ребре. Функции, обрабатывающие данные события, реализованы с помощью языка программирования JavaScript. На рисунке 3 продемонстрировано поведение программы при нажатии на связь между узлами графа. Подсвечивается выбранное ребро, появляется информация о том, от кого и к кому ведет данная связь, а также о значении в заданной метрике. Например, на данном рисунке показано, что Пользователь 1 поставил Пользователю 2 шесть лайков. Кроме того, приложение поддерживает возможность перехода на его страницу в социальной сети при нажатии на фото пользователя. Работа продемонстрирована на рисунке 4.

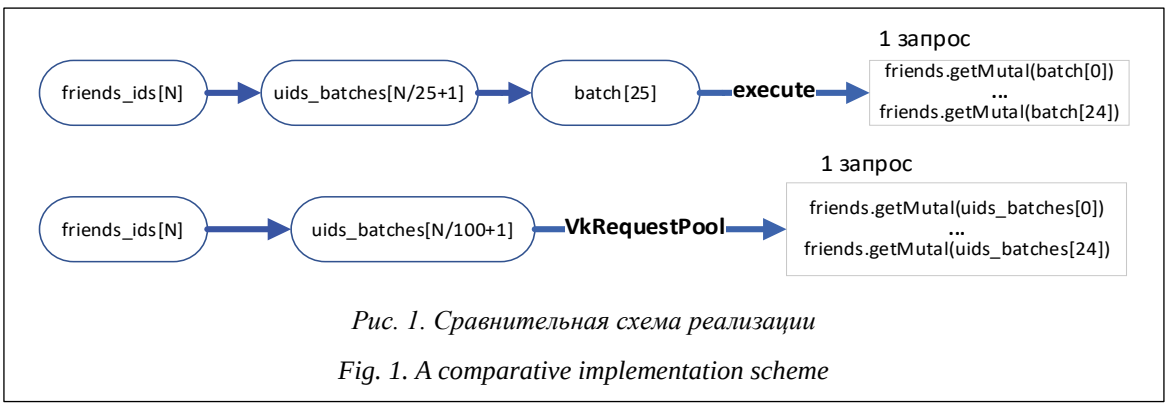

Рис. 1. Сравнительная схема реализации

Fig. 1. A comparative implementation scheme

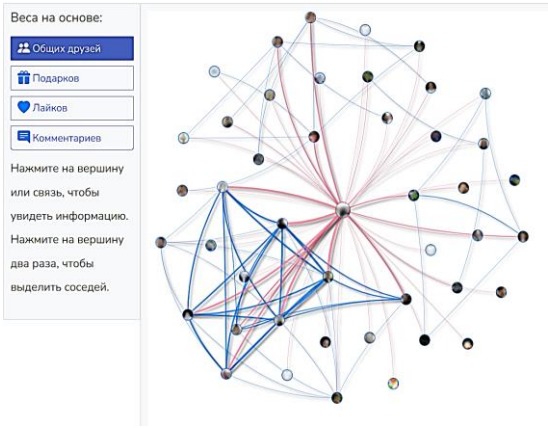

Рис. 2. Скриншот экрана с построенным социальным графом (для сохранения конфиденциальности аватары пользователей размыты)

Fig. 2. A screenshot of the built social graph (user avatars are blurred to preserve privacy)

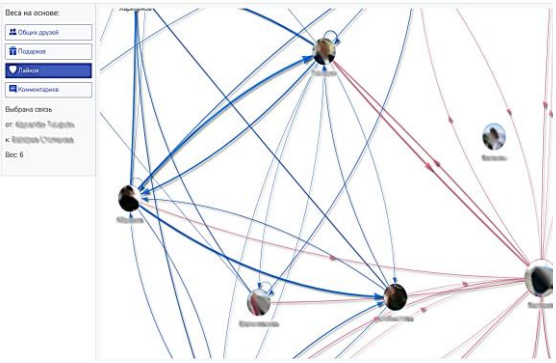

Рис. 3. Отображение статистики взаимодействия между пользователями

Fig. 3. A user interaction statistics

Для взаимодействия с графом также реализована функция, которая позволяет двойным кликом на вершину выделить инцидентные ей ребра, временно перекрасив их в серый цвет. Для выхода из данного режима нужно дважды нажать на поле с графом в место, отличное от какой-либо из вершин.

Выводы и дискуссия

Результаты построения социального графа пользователей в социальной сети «ВКонтакте» вносят существенный вклад в создание комплексного инструмента, направленного на снижение рисков, связанных с социоинженерными атаками. С помощью данного инструмента лица, принимающие решения, могут спрогнозировать свои оценки распространения многоходовой социоинженерной атаки и предпринять меры по их снижению. Кроме того, инструмент дает возможность оценить в целом интенсивность коммуникации сотрудников в организации. Разработанный прототип является удачным базисом для дальнейших надстроек, носящих более комплексный характер и направленных на оценку защищенности персонала организации от социоинженерных атак, выработку рекомендаций по принятию мер, снижающих риски. К преимуществам разработанного инструмента по сравнению с предложенным в [18] можно отнести оптимизацию функции для сбора информации об общих друзьях пользователя, добавление расчета метрик взаимодействия между пользователями, улучшение функциональности и визуализации построения социального графа путем добавления большего числа сведений о взаимодействии пользователей.

Вместе с тем остаются актуальными задачи, определяющие дальнейшие перспективы исследований, например, выделение на социальном графе наиболее вероятных и критичных путей распространения многоходовых социоинженерных атак в соответствии с разработанными ранее методами и моделями [14, 15]. В дальнейшем приложение может быть расширено до функциональности, востребованной в конкретном приложении. Это могут быть не только разработки, направленные на противодействие социоинженерным атакам, но и социологические исследования для изучения интенсивности взаимодействия пользователей, маркетинговые исследования для выявления возможности продвижения продукта в отдельных социальных группах, зависимости между интенсивностью взаимодействия пользователей и востребованностью товара в определенной группе и т.п.

Дальнейшими направлениями развития разработки могут быть дополнение ее новой функциональностью, такой как внедрение визуализации в соответствии с кластеризацией интересов пользователей (подписка на одни сообщества, репосты постов из одних сообществ) [19], выявление влиятельных узлов в графе, через которые наиболее эффективно распространение информации [20–21], их визуализация [22, 23]; комбинирование методов анализа текста, изображений и социального графа для проведения углубленного исследования взаимодействия пользователей [24, 25].

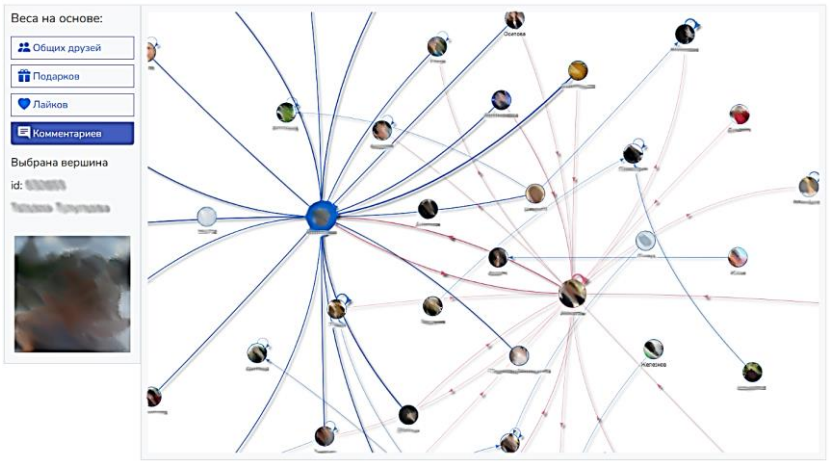

Рис. 4. Действие при нажатии на вершину социального графа

Fig. 4. An action when clicking on the top of the social graph

Близкой к рассмотренной проблеме является задача прогнозирования распространения слухов. Так, для последующих исследований могут быть использованы полученные в [26–28] результаты, касающиеся моделирования процесса принятия решений пользователем о передаче информации (слуха). Кроме того, для оптимизации анализа графов могут быть полезны методы интеллектуального уменьшения плотности графов [29, 30] или методы параллельного разбиения [31], применение которых позволило бы уменьшить вычислительную сложность при анализе огромного количества данных. В планах дальнейших исследований – построение графа на основе объединенной информации, извлекаемой из социальных сетей «ВКонтакте» и «Одноклассники» [32, 33].

Заключение

Разработанное приложение дает возможность строить социальный граф пользователя на основе выбранной метрики взаимодействия друзей. Оно содержит удобные инструменты для взаимодействия с ним, что делает достижимой цель исследования – повышение доступности анализа защищенности от многоходовых социоинженерных атак за счет создания инструмента для визуализации социального графа пользователей «ВКонтакте».

Практическая значимость исследования заключается в создании инструмента, позволяющего лицам, принимающим решения, выявлять наиболее реальные сценарии распространения социоинженерных атак, что даст возможность принимать меры по снижению вероятности их реализации и оперативнее расследовать уже случившиеся инциденты.

Новизна исследования в построении социального графа пользователя «ВКонтакте» с отображением различных метрик интенсивности его взаимодействия с друзьями и их между собой, которые могут быть использованы при выявлении уязвимостей к многоходовым социоинженерным атакам.

Работа выполнена в рамках проекта по госзаданию СПИИ РАН № FFZF-2022-0003;
при финансовой поддержке РФФИ, проект № 20-07-00839, грант Президента МК-5237.2022.1.6.

Литература

1. Siddiqi M.A., Pak W., Siddiqi M.A. A study on the psychology of social engineering-based cyberattacks and existing countermeasures. Applied Sciences, 2022, vol. 12, no. 12, art. 6042. DOI: 10.3390/app12126042.
2. Washo A.H. An interdisciplinary view of social engineering: A call to action for research. Computers in Human Behavior Reports, 2021, vol. 4, art. 100126. DOI: 10.1016/j.chbr.2021.100126.
3. Astakhova L.V., Medvedev I.A. An information tool for increasing the resistance of employees of an organization to social engineering attacks. Sci. and Tech. Inf. Proc., 2021, vol. 48, no. 1, pp. 15–20. DOI: 10.3103/S0147688221010020.
4. Абрамов М.В., Тулупьева Т.В., Тулупьев А.Л. Социоинженерные атаки: социальные сети и оценки защищенности пользователей. СПб: Изд-во ГУАП, 2018. 266 с.
5. Grassegger T., Nedbal D. The role of employees' information security awareness on the intention to resist social engineering. Procedia Comp. Sci., 2021, vol. 181, pp. 59–66. DOI: 10.1016/j.procs.2021.01.103.
6. Khlobystova A.O., Tulupyeva T.V., Maksimov A.G., Korepanova A.A. An approach to quantification of relationship types between users based on the frequency of combinations of non-numeric evaluations. In: AISC. Proc. IITI, 2019, pp. 206–213. DOI: 10.1007/978-3-030-50097-9_21.

7. Vega L., Mendez-Vazquez A., López-Cuevas A. Probabilistic reasoning system for social influence analysis in online social networks. Soc. Network Analysis and Mining, 2021, vol. 11, no. 1, pp. 1–20. DOI: 10.1007/s13278-020-00705-z.

8. Karanatsiou D., Sermpezis P., Gruda D., Kafetsios K., Dimitriadis I., Vakali A. My tweets bring all the traits to the yard: Predicting personality and relational traits in online social networks. ACM TWEB, 2022, vol. 16, no. 2, pp. 1–26. DOI: 10.1145/3523749.

9. Piao Y., Ye K., Cui X. Privacy inference attack against users in online social networks: A literature review. IEEE Access, 2021, vol. 9, pp. 40417–40431. DOI: 10.1109/access.2021.3064208.

10. Leonov P.Y., Vorobyev A.V., Ezhova A.A., Kotelyanets O.S., Zavalishina A.K., Morozov N.V. The main social engineering techniques aimed at hacking information systems. Proc. USBEREIT, 2021, pp. 0471–0473. DOI: 10.1109/USBEREIT51232.2021.9455031.

11. Syafitri W., Shukur Z., Mokhtar U.A., Sulaiman R., Ibrahim M.A. Social engineering attacks prevention: A systematic literature review. IEEE Access, 2022, pp. 39325–39343. DOI: 10.1109/ACCESS.2022.3162594.

12. Тулупьева Т.В. Психологические аспекты информационной безопасности организации в контексте социоинженерных атак // Управленческое консультирование. 2022. Т. 2. № 158. С. 123–138. DOI: 10.22394/1726-1139-2022-2-123-138.

13. Abe N., Soltys M. Deploying health campaign strategies to defend against social engineering threats. Procedia Comp. Sci., 2019, vol. 159, pp. 824–831. DOI: 10.1016/j.procs.2019.09.241.

14. Khlobystova A., Abramov M., Tulupyev A. Employees' social graph analysis: A model of detection the most criticality trajectories of the social engineering attack's spread. In: AISC. Proc. IITI, 2019, pp. 198–205. DOI: 10.1007/978-3-030-50097-9_20.

15. Khlobystova A., Abramov M., Tulupyev A. An approach to estimating of criticality of social engineering attacks traces. In: SSDC. Proc. ICIT, 2019, pp. 446–456. DOI: 10.1007/978-3-030-12072-6_36.

16. Ngo D.T., Cao C.-N., Hoang Ph.-L. et al. Identifying micro-influencers on social media using user graph construction approach. Proc. XIII Int. Conf. KSE, 2021, pp. 1–6. DOI: 10.1109/KSE53942.2021.9648780.

17. Khlobystova A., Abramov M., Korepanova A., Liapin N. Identification of predictors for estimation the intensity of relationships between users of online social networks. Proc. VI Int. Sci. Conf. IITI, 2023, vol. 566, pp. 216–225. DOI: 10.1007/978-3-031-19620-1_21.

18. Олисеенко В.Д., Абрамов М.В., Тулупьев А.Л., Иванов К.А. Прототип программного комплекса для анализа аккаунтов пользователей социальных сетей: веб-фреймворк Django // Программные продукты и системы. 2022. Т. 35. № 1. С. 45–53.

19. Trolliet T., Cohen N., Giroire F., Hogie L., Perennes S. Interest clustering coefficient: A new metric for directed networks like Twitter. J. of Complex Networks, 2022, vol. 10, no. 1, art. cnab030. DOI: 10.1093/comnet/cnab030.

20. Norfarah N., Siti-Nabiha A.K., Samsudin M.A. Social network analysis to identify influencer in twitter conversation on SMEs in times of covid-19 pandemic. Proc. ICBT, 2022, pp. 439–452. DOI: 10.1007/978-3-031-08087-6_31.

21. Loucif H., Akhrouf S. A new recursive model to measure influence in subscription social networks: A case study using Twitter. Proc. IC-AIRES, 2021, pp. 518–526. DOI: 10.1007/978-3-030-92038-8_52.

22. Mussiraliyeva S., Baispay G., Ospanov R., Medetbek Z., Shalabayev K. Graphical visualization of the connections of involved users and identifying influential spreaders in a social network. Proc. ICEEE, 2022, pp. 311–315. DOI: 10.1109/ICEEE55327.2022.9772556.

23. Alsaif S.A., Hidri A., Hidri M.S. Towards inferring influential Facebook users. Computers, 2021, vol. 10, no. 5, p. 62. DOI: 10.3390/computers10050062.

24. Wang A., Potika K. Cyberbullying classification based on social network analysis. Proc. IEEE VII Int. Conf. BigDataService, 2021, pp. 87–95. DOI: 10.1109/BigDataService52369.2021.00016.

25. Jayakody J., Jayatilake N. Comparison Analysis and Data Retrieval to identify the associated people in social media by Image Processing. Proc. II ICARC, 2022, pp. 137–141. DOI: 10.1109/ICARC54489.2022.9753754.

26. Liu W., Wang J., Ouyang Y. Rumor transmission in online social networks under Nash equilibrium of a psychological decision game. Networks and Spatial Economics, 2022, vol. 22, no. 4, pp. 1–24. DOI: 10.1007/s11067-022-09574-9.

27. Hosseini S., Zandvakili A. Information dissemination modeling based on rumor propagation in online social networks with fuzzy logic. Social Network Analysis and Mining, 2022, vol. 12, art. 34. DOI: 10.1007/s13278-022-00859-y.

28. Devarapalli R.K., Biswas A. Rumor detection and tracing its source to prevent cyber-crimes on social media. In: Intelligent Data Analytics for Terror Threat Prediction: Architectures, Methodologies, Techniques and Applications, 2021, pp. 1–30. DOI: 10.1002/9781119711629.ch1.

29. Bhattacharya I., Gupta S. Intelligent friendship graphs: A theoretical framework. Proc. Int. Conf. Soft Computing and its Engineering Applications, 2022, pp. 90–102. DOI: 10.1007/978-3-031-05767-0_8.

30. Bartal A., Ravid G. Analyzing a large and unobtainable relationship graph using a streaming activity graph. Inf. Sci., 2021, vol. 546, pp. 1097–1112. DOI: 10.1016/j.ins.2020.09.063.

31. Lopes T., Stroele V., Dantas M., Braga R., Mehaut J.F. A parallel graph partitioning approach to enhance community detection in social networks. Proc. ISCC, 2020, pp. 1–6. DOI: 10.1109/ISCC50000.2020.9219602.

32. Korepanova A.A., Oliseenko V.D., Abramov M.V. Applicability of similarity coefficients in social circle matching. Proc. XXIII Int. Conf. SCM, 2020, pp. 41–43. DOI: 10.1109/SCM50615.2020.9198782.

33. Корепанова А.А., Абрамов М.В., Тулупьев А.Л. Идентификация аккаунтов пользователей социальных сетей при помощи сравнения графического контента // Научн.-технич. вестн. информационных технологий, механики и оптики. 2021. Т. 21. № 6. С. 942–950. DOI: 10.17586/2226-1494-2021-21-6-942-950.

Software & Systems
DOI: 10.15827/0236-235X.141.097-106

Received 28.09.22, Revised 25.11.22
2023, vol. 36, no. 1, pp. 097–106

Developing a software tool for constructing a social graph of a social network user in the task of analyzing its security from multi-pass social engineering attacks

A.O. Khlobystova [1], *Junior Researcher, aok@dscs.pro*
M.V. Abramov [1], *Ph.D. (Engineering), Head of Laboratory, mva@dscs.pro*
V.A. Sazanov [2], *Student, mail@dscs.pro*

[1] *St. Petersburg Federal Research Center of the Russian Academy of Sciences, Laboratory of Theoretical and Interdisciplinary Problems of Informatics, St. Petersburg, 199178, Russian Federation*
[2] *St. Petersburg State University, St. Petersburg, 199034, Russian Federation*

Abstract. The study is based on the problem of lacking visualization tools showing the intensity of interaction between users of the VK online social network, namely the display of metrics that allow evaluating and ranking the intensity of interaction both between a user and his friends, and between friends with each other.

The aim of this paper is to improve the accessibility and timeliness of users' interaction intensity analysis by automating social graph visualization. It is assumed that the numerical coefficients of the social graph arcs will be compared with an assessment of user interaction intensity based on data extracted from publicly available sources of the VK social network.

To achieve this goal, the authors considered the following issues: optimization of aggregating necessary data on observed interaction of friends in the VK social network, software implementation of functions for building a social graph, visualization of users' interaction intensity with the possibility of choosing metrics of interest, creation of convenient interface and embedding the developed toolkit into a web-application.

The subject of the research is the data of interaction between VK users and the ways of their visualization. The research methods are based on optimizing sending queries to VK API, as well as developing functions and settings to build a social graph.

The theoretical significance of the proposed solution is in the development of approaches to analyze the proliferation of multistep social engineering attacks and to validate models for estimating user interaction intensity. The result has significant practical relevance consisting in automating the process of assessing the intensity of employee interaction, thereby laying the foundation for taking effective measures to mitigate the risks of successful social engineering attacks. The novelty of the research is in the proposed improvement of visualization of VK users' social graph construction by adding new metrics to assess the intensity of users' interaction.

Keywords: social graph, social engineering attacks, spread probability estimate, interaction visualization, online social networks, web application, information security, user interaction intensity metrics, web application architecture for building the social graph.

Acknowledgements. *This work was carried out within the framework of the project under the state assignment of SPC RAS SPIIRAS FFZF-2022-0003; with the financial support of the RFBR, project no. 20-07-00839, the President's grant MK-5237.2022.1.6.*

References

1. Siddiqi M.A., Pak W., Siddiqi M.A. A study on the psychology of social engineering-based cyberattacks and existing countermeasures. *Applied Sciences*, 2022, vol. 12, no. 12, art. 6042. DOI: 10.3390/app12126042.
2. Washo A.H. An interdisciplinary view of social engineering: A call to action for research. *Computers in Human Behavior Reports*, 2021, vol. 4, art. 100126. DOI: 10.1016/j.chbr.2021.100126.
3. Astakhova L.V., Medvedev I.A. An information tool for increasing the resistance of employees of an organization to social engineering attacks. *Sci. and Tech. Inf. Proc.*, 2021, vol. 48, no. 1, pp. 15–20. DOI: 10.3103/S0147688221010020.
4. Abramov M., Tulupyeva T., Tulupyev A. *Social Engineering Attacks: Social Networks and User Security Estimates*. St. Petersburg, 2018, 266 p. (in Russ.).
5. Grassegger T., Nedbal D. The role of employees' information security awareness on the intention to resist social engineering. *Procedia Comp. Sci*., 2021, vol. 181, pp. 59–66. DOI: 10.1016/j.procs.2021.01.103.
6. Khlobystova A.O., Tulupyeva T.V., Maksimov A.G., Korepanova A.A. An approach to quantification of relationship types between users based on the frequency of combinations of non-numeric evaluations. In: *AISC. Proc. IITI*, 2019, pp. 206–213. DOI: 10.1007/978-3-030-50097-9_21.
7. Vega L., Mendez-Vazquez A., López-Cuevas A. Probabilistic reasoning system for social influence analysis in online social networks. *Soc. Network Analysis and Mining*, 2021, vol. 11, no. 1, pp. 1–20. DOI: 10.1007/s13278-020-00705-z.
8. Karanatsiou D., Sermpezis P., Gruda D., Kafetsios K., Dimitriadis I., Vakali A. My tweets bring all the traits to the yard: Predicting personality and relational traits in online social networks. *ACM TWEB*, 2022, vol. 16, no. 2, pp. 1–26. DOI: 10.1145/3523749.
9. Piao Y., Ye K., Cui X. Privacy inference attack against users in online social networks: A literature review. *IEEE Access*, 2021, vol. 9, pp. 40417–40431. DOI: 10.1109/access.2021.3064208.
10. Leonov P.Y., Vorobyev A.V., Ezhova A.A., Kotelyanets O.S., Zavalishina A.K., Morozov N.V. The main social engineering techniques aimed at hacking information systems. *Proc. USBEREIT*, 2021, pp. 0471–0473. DOI: 10.1109/USBEREIT51232.2021.9455031.
11. Syafitri W., Shukur Z., Mokhtar U.A., Sulaiman R., Ibrahim M.A. Social engineering attacks prevention: A systematic literature review. *IEEE Access*, 2022, pp. 39325–39343. DOI: 10.1109/ACCESS.2022.3162594.
12. Tulupieva T.V. Psychological aspects of the organization's information security in the context of socio-engineering attacks. *Administrative Consulting*, 2022, vol. 2, no. 158, pp. 123–138. DOI: 10.22394/1726-1139-2022-2-123-138 (in Russ.).
13. Abe N., Soltys M. Deploying health campaign strategies to defend against social engineering threats. *Procedia Comp. Sci.*, 2019, vol. 159, pp. 824–831. DOI: 10.1016/j.procs.2019.09.241.
14. Khlobystova A., Abramov M., Tulupyev A. Employees' social graph analysis: A model of detection the most criticality trajectories of the social engineering attack's spread. In: *AISC. Proc. IITI*, 2019, pp. 198–205. DOI: 10.1007/978-3-030-50097-9_20.
15. Khlobystova A., Abramov M., Tulupyev A. An approach to estimating of criticality of social engineering attacks traces. In: *SSDC. Proc. ICIT*, 2019, pp. 446–456. DOI: 10.1007/978-3-030-12072-6_36.
16. Ngo D.T., Cao C.-N., Hoang Ph.-L. et al. Identifying micro-influencers on social media using user graph construction approach. *Proc. XIII Int. Conf. KSE*, 2021, pp. 1–6. DOI: 10.1109/KSE53942.2021.9648780.
17. Khlobystova A., Abramov M., Korepanova A., Liapin N. Identification of predictors for estimation the intensity of relationships between users of online social networks. *Proc. VI Int. Sci. Conf. IITI*, 2023, vol. 566, pp. 216–225. DOI: 10.1007/978-3-031-19620-1_21.
18. Oliseenko V.D., Abramov M.V., Tulupyev A.L., Ivanov K.A. A software package prototype for analyzing user accounts in social networks: Django web framework. *Software & Systems*, 2022, vol. 35, no. 1, pp. 45–53 (in Russ.).
19. Trolliet T., Cohen N., Giroire F., Hogie L., Perennes S. Interest clustering coefficient: A new metric for directed networks like Twitter. *J. of Complex Networks*, 2022, vol. 10, no. 1, art. cnab030. DOI: 10.1093/comnet/cnab030.
20. Norfarah N., Siti-Nabiha A.K., Samsudin M.A. Social network analysis to identify influencer in twitter conversation on SMEs in times of covid-19 pandemic. *Proc. ICBT*, 2022, pp. 439–452. DOI: 10.1007/978-3-031-08087-6_31.
21. Loucif H., Akhrouf S. A new recursive model to measure influence in subscription social networks: A case study using Twitter. *Proc. IC-AIRES*, 2021, pp. 518–526. DOI: 10.1007/978-3-030-92038-8_52.
22. Mussiraliyeva S., Baispay G., Ospanov R., Medetbek Z., Shalabayev K. Graphical visualization of the connections of involved users and identifying influential spreaders in a social network. *Proc. ICEEE*, 2022, pp. 311–315. DOI: 10.1109/ICEEE55327.2022.9772556.

23. Alsaif S.A., Hidri A., Hidri M.S. Towards inferring influential Facebook users. *Computers*, 2021, vol. 10, no. 5, pp. 62. DOI: 10.3390/computers10050062.

24. Wang A., Potika K. Cyberbullying classification based on social network analysis. *Proc. IEEE VII Int. Conf. BigDataService*, 2021, pp. 87–95. DOI: 10.1109/BigDataService52369.2021.00016.

25. Jayakody J., Jayatilake N. Comparison Analysis and Data Retrieval to identify the associated people in social media by Image Processing. *Proc. II ICARC*, 2022, pp. 137–141. DOI: 10.1109/ICARC54489.2022.9753754.

26. Liu W., Wang J., Ouyang Y. Rumor transmission in online social networks under Nash equilibrium of a psychological decision game. *Networks and Spatial Economics*, 2022, vol. 22, no. 4, pp. 1–24. DOI: 10.1007/s11067-022-09574-9.

27. Hosseini S., Zandvakili A. Information dissemination modeling based on rumor propagation in online social networks with fuzzy logic. *Social Network Analysis and Mining*, 2022, vol. 12, art. 34. DOI: 10.1007/s13278-022-00859-y.

28. Devarapalli R.K., Biswas A. Rumor detection and tracing its source to prevent cyber-crimes on social media. In: *Intelligent Data Analytics for Terror Threat Prediction: Architectures, Methodologies, Techniques and Applications*, 2021, pp. 1–30. DOI: 10.1002/9781119711629.ch1.

29. Bhattacharya I., Gupta S. Intelligent friendship graphs: A theoretical framework. *Proc. Int. Conf. Soft Computing and its Engineering Applications*, 2022, pp. 90–102. DOI: 10.1007/978-3-031-05767-0_8.

30. Bartal A., Ravid G. Analyzing a large and unobtainable relationship graph using a streaming activity graph. *Inf. Sci.*, 2021, vol. 546, pp. 1097–1112. DOI: 10.1016/j.ins.2020.09.063.

31. Lopes T., Stroele V., Dantas M., Braga R., Mehaut J.F. A parallel graph partitioning approach to enhance community detection in social networks. *Proc. ISCC*, 2020, pp. 1–6. DOI: 10.1109/ISCC50000.2020.9219602.

32. Korepanova A.A., Oliseenko V.D., Abramov M.V. Applicability of similarity coefficients in social circle matching. *Proc. XXIII Int. Conf. SCM*, 2020, pp. 41–43. DOI: 10.1109/SCM50615.2020.9198782.

33. Korepanova A.A., Abramov M.V., Tulupyev A.L. Social media user identity linkage by graphic content comparison. *Sci.Tech. J. Inf. Technol. Mech. Opt.*, 2021, vol. 136, no. 6, pp. 942–950. DOI: 10.17586/2226-1494-2021-21-6-942-950 (in Russ.).

Для цитирования

Хлобыстова А.О., Абрамов М.В., Сазанов В.А. Разработка программного инструмента для построения социального графа пользователя социальной сети в задаче анализа его защищенности от многоходовых социоинженерных атак // Программные продукты и системы. 2023. Т. 36. № 1. С. 097–106. DOI: 10.15827/0236-235X.141.097-106.

For citation

Khlobystova A.O., Abramov M.V., Sazanov V.A. Developing a software tool for constructing a social graph of a social network user in the task of analyzing its security from multi-pass social engineering attacks. *Software & Systems*, 2023, vol. 36, no. 1, pp. 097–106 (in Russ.). DOI: 10.15827/0236-235X.141.097-106.