

Оценка степени открытости пользователя социальной сети с применением экспертной модели на основе байесовской сети доверия

М. С. Фролова

Санкт-Петербургский государственный университет
m.f.26@mail.ru

А. А. Корепанова

Федеральное государственное бюджетное учреждение
науки «Санкт-Петербургский Федеральный
исследовательский центр Российской академии наук»
(СПб ФИЦ РАН)
aak@dscs.pro

М.В. Абрамов

Федеральное государственное бюджетное учреждение
науки «Санкт-Петербургский Федеральный
исследовательский центр Российской академии наук»
(СПб ФИЦ РАН)
mva@dscs.pro

Аннотация. Одной из самых актуальных проблем информационной безопасности в настоящее время является предотвращение успешных инцидентов социоинженерных атак — психологического манипулирования людьми с целью получения доступа к конфиденциальной информации. Для оценки уязвимости пользователя информационной системы к такому типу атак необходимо оценить его личностные особенности. Перспективной в данном направлении является оценка степени открытости (открытость рассматривается согласно фактору “открытости опыту”, входящему в модель личности “The Big Five”) пользователя социальной сети. В данной работе рассмотрен подход к оценке открытости пользователя социальной сети с помощью байесовской сети доверия. На основе пятифакторного опросника личности рассмотрены характеристики, которые можно извлечь со страницы пользователя, потенциально влияющие на его открытость к принятию информации. Предложена структура байесовской сети доверия для решения данной задачи.

Ключевые слова: социоинженерная атака; социальная сеть; байесовские сети; байесовская сеть доверия.

I. ВВЕДЕНИЕ

В настоящее время зачастую в различных сферах производства и в сфере услуг важные документы хранятся в электронном виде в информационной системе. Злоумышленники получить доступ к этой информации извне могут либо попытавшись взломать систему информационной безопасности предприятия, либо через сотрудников данного предприятия, имеющих доступ к необходимым данным. В связи с этим большую угрозу для безопасности фирмы представляют социоинженерные атаки — набор прикладных психологических и аналитических приемов манипулирования психическим

сознанием человека, которые злоумышленники применяют для скрытой мотивации пользователей публичной или корпоративной сети к нарушениям устоявшихся правил и политик в области информационной безопасности [31].

С каждым годом социоинженерные атаки совершенствуются, что требует постоянного развития существующих методов защиты [27], при разработке которых необходимо ориентироваться именно на личностные особенности пользователей системы.

Для разработки программного аппарата с целью предотвращения положительных исходов социоинженерных атак удобным инструментом является профиль уязвимости пользователя — совокупность психологических и поведенческих особенностей сотрудника фирмы, потенциально влияющих на исход направленных на него социоинженерных атак [7]. Данная работа посвящена усовершенствованию метода составления профиля уязвимости пользователя к социоинженерным атакам за счёт оценки открытости пользователя. Исследование основано на модели Большой Пятерки (The Big Five) [20]. Пятифакторная модель — это модель личности, позволяющая описать человека при помощи 5 черт, или, иначе говоря, факторов. Шкала «открытость новому опыту» (в данной работе исследуется именно она), показывает, насколько человек заинтересован в расширении собственных горизонтов, узнавании нового, получение новой информации. Таким образом данная работа посвящена оценке степени открытости пользователя в контексте одноименного фактора Большой Пятерки.

Многие исследования показывают положительную корреляцию между открытостью пользователя опыту и

уязвимостью к различным видам манипуляции и социоинженерным атакам [39, 15]. Поэтому получение данной оценки является перспективной задачей в разработке аппарата защиты информационных систем от угроз злоумышленников. Чтобы осуществить необходимую оценку удобно использовать информацию, которую сам же пользователь размещает на своих страницах в социальных сетях, а также данные о его реакциях на посты в новостной ленте. Эта информация легко доступна, так что может быть потенциально использована злоумышленником. Данные в социальных сетях отличаются нечёткостью и неполнотой, поэтому в данной работе для решения поставленной задачи оценки используются байесовские сети доверия, они являются удобным инструментом для разработки моделей с причинно-следственными связями для ответов на вероятностные вопросы, а также позволяют работу с неполными данными.

Результаты, полученные в данной работе, полезны для дальнейших исследований, посвящённых повышению защищённости информационных систем от социоинженерных атак, для разработки методов защиты от них на основе профиля уязвимостей пользователя.

II. ОБЗОР ЛИТЕРАТУРЫ

Данная работа выполняется в рамках общего исследования, посвященного анализу уязвимости пользователей информационных систем к социоинженерным атакам с целью разработки программного обеспечения для предотвращения успешных инцидентов [6]. В работе [12] предлагается схема развития социоинженерной атаки, рассмотрены зависимости исходов атаки от действий злоумышленников и ответных реакций пользователей, а также предложена иерархия информационных моделей, включающая в себя информационные объекты (документы), пользователей, вероятные атакующие воздействия [17].

Одним из важнейших направлений для решения проблемы повышения защищенности пользователей информационных систем от социоинженерных атак является построение профиля уязвимостей пользователя. В работах [8, 9] подчеркивается важность построения психологического профиля, отражающего степень выраженности психологических особенностей пользователя, и приводятся наработки в этой области. Существуют различные подходы в области анализа выраженности психологических особенностей пользователя, например, психологическое тестирование или анализ личной информации на странице пользователя в социальной сети [14, 16, 18, 19]. В работе [14] на основе цифрового следа пользователя социальной сети оцениваются его личностные особенности, а также в результате сравнения “человеческой” и “компьютерной” оценки психологических особенностей установлено, что “компьютерная” оценка обладает более высокой точностью.

Одной из наиболее комплексных и подробных систем для оценки личностных особенностей человека, в том числе необходимой для данного исследования “открытости

новому опыту”, является “Большая Пятёрка”. В работе [31] автор подробно раскрывает обоснованность использования именно этого тестирования для получения наиболее точных знаний о поведении и склонностях человека, а также проводит взаимосвязь между полученными показателями по определенным факторам теста и склонностью человека быть более открытым к информации извне.

Существуют исследования, показывающие связь между открытостью и различными характеристиками поведения пользователя в социальной сети [38]. В исследовании [5] проводилась оценка корреляции между факторами большой пятёрки и активностью пользователя в социальных сетях. Согласно этому исследованию, открытость опыту положительно коррелировала с числом записей на стене пользователя и количеством его друзей в социальной сети.

Удобной математической моделью для работы с полученной информацией являются байесовские сети [4], которые имеют множество приложений, среди которых решение задач в области информационной безопасности и социоинженерных атак, например, для оценки интенсивности поведения пользователя социальной сети на примере постинга [10], [11]. В работе [13] предложены подходы к моделированию социоинженерных атак на пользователя, основанные на байесовских сетях доверия. В работе [29] исследуется возможность использования байесовских сетей для построения аппарата диагностики социального тревожного расстройства у студентов. Авторы приходят к заключению, что данный математический инструмент является очень адаптивным, позволяет представить информацию в простой и удобной форме, существенно снижает вычислительную сложность, позволяет добиться высокой точности расчетов.

III. ПОСТАНОВКА ЗАДАЧИ

Цель данной работы — разработать метод оценки открытости пользователя социальной сети по пятифакторной модели личности и автоматизировать его. Для достижения поставленной цели необходимо получить данные из профиля пользователя социальной сети: число групп в его подписках, число его друзей; наличие информации в графах “статус”, “о себе”, “занятия”, “книги”, “цитаты”, “интересы”, “вдохновение”, “главное в людях”, “главное в жизни”. Следует выделить ряд критериев, по которым будет происходить оценка, и, на основе пятифакторного опросника, составить математическую модель, отражающую результаты исследования. В данной работе было решено использовать байесовскую сеть доверия — графическую структуру для представления вероятностных отношений между большим количеством переменных и для осуществления вероятностного вывода на основе этих переменных [3]. Данная модель позволяет работать с неполными данными. Для означивания разработанной математической модели необходимо написать парсер-программу и собрать данные о пользователях ВКонтакте, на основе которых необходимо вычислить средние показатели по каждому фактору в модели.

IV. ОПИСАНИЕ МОДЕЛИ

В результате работы был предложен прототип модели, устройство которой описано ниже, данная модель призвана оценить открытость пользователя с помощью анализа данных, доступных в социальной сети. В работе происходит оценка на основе некоторых численных характеристик, которые можно напрямую получить со страницы пользователя в социальной сети. Для оценки открытости пользователя были выбраны следующие характеристики, отражающие активность его взаимодействия с социальной сетью: частота “лайканья”, а именно количество отметок “нравится”, которыми пользователь оценивает потребляемый контент, за определенный промежуток времени; частота постинга — туда включается частота размещения собственных постов на странице и частота репостов записей различных сообществ и других пользователей; число друзей; количество личной информации в профиле; количество групп в подписках. Для оценки количества личной информации на страничке использовались данные о заполнении/не заполнении пользователем ВКонтакте полей из разделов “Интересы” и “Жизненная позиция”, а именно: статус, о себе, деятельность, интересы, любимые книги, любимые цитаты, источники вдохновения, главное в жизни, главное в людях. Анализировалось наличие именно вышеперечисленных полей, так как, предположительно, они глубже отражают информацию о личностных особенностях пользователя, в отличие от разделов “Контакты”, “Образование” или “Карьера”. То есть их заполнение может свидетельствовать о желании данного пользователя рассказать о своих интересах и жизненных приоритетах другим, из наличия которого можно сделать косвенный вывод о его психологических особенностях (экстраверсии/интроверсии) [32]. Данным характеристикам соответствуют переменные в байесовской сети доверия. Каждая переменная может принимать одно из следующих значений: “Низкое”, “Высокое”. Кроме численных характеристик, в перспективе полезным может оказаться анализ сфер интересов пользователя по потребляемому им контенту. Согласно предположению, наличие большого количества групп с новостным контентом, рекламными объявлениями (как и наличие на страничке пользователя репостов с подобными записями) может свидетельствовать о высокой степени открытости к новому опыту, в то время как небольшое число групп с узконаправленной спецификой говорит о закрытости пользователя к информации, не связанной с интересующей его тематикой. В данной работе при практической оценке используется только информация о количестве групп в подписках пользователя, в дальнейшем планируется также анализировать и их тематику.

Предложенная модель степени открытости пользователя приведена на рисунке 1.



Рис. 1. Степень открытости пользователя

Вышеописанная модель универсальна для проведения необходимой оценки на основе профиля пользователя в любой из существующих социальных сетей (ВКонтакте, Instagram, Facebook, Twitter, Одноклассники etc.). В данной работе анализ происходит на основе страниц пользователей в социальной сети ВКонтакте.

V. ОЗНАЧИВАНИЕ ПЕРЕМЕННЫХ

Предложенная модель сети — бинарная, т. е. в каждый узел может принимать одно из двух значений. Для осуществления расчетов необходимо составить соответствие численных показателей бинарным показателям в узлах сети. При переводе числовых характеристик в бинарные для каждой характеристики в качестве пороговых значений использовались средние численные показатели пользователей социальной сети “ВКонтакте”, которые вычислялись на основе данных о 100 пользователях, имеющих менее 150 друзей и 100 групп в подписках, дабы облегчить сбор данных. С целью получения более усредненного результата для каждого пользователя, частота “лайканья” высчитывалась следующим образом: количество “лайков”, оставленных пользователем на записях его друзей и его групп в подписках за 3 дня делилось на 3. Для вычисления частоты постинга используется временной промежуток длиной в неделю, выбранный экспериментальным образом. Данное соответствие приведено в таблице 1.

Таблица 1 Перевод численных показателей в бинарные

	Низкое	Высокое
Количество друзей	≤ 71 человек	> 71 человек
Частота постинга	1 пост за неделю	> 1 поста за неделю
Частота “лайканья”	≤ 4 “лайков” за день	> 4 “лайков” за день
Количество личной информации на странице	≤ 2 единиц	> 2 единиц
Группы в подписках	≤ 52 группы	> 52 группы

а. Перевод численных показателей в бинарные

На данном этапе условные вероятности в сети доверия проставлялись экспертно. На основе предложенной модели с использованием полученных средних показателей по каждому критерию на языке C# было написано приложение, которое по Id пользователя ВКонтакте собирает необходимые данные и с помощью библиотеки Smile для работы с байесовскими сетями осуществляет нужную оценку.

В таблице 2 приведен пример оценки модели на основе информации о трёх пользователях:

ТАБЛИЦА 2. Степень открытости пользователей сети ВКонтакте

	Число друзей	Ч-та постинга	Ч-та лайканья	Кол-во личной информации на странице	Число групп в подписках	Степень открытости:
1	148	0	0	0	68	Высокая: 0,262 Низкая: 0,738
2	51	0	1	0	53	Высокая: 0,092 Низкая: 0,908
3	132	0	10	2	64	Высокая: 0,768 Низкая: 0,232

а. Степень открытости пользователей сети ВКонтакте

VI. ЗАКЛЮЧЕНИЕ

В данной работе представлен прототип модели оценки открытости пользователя новому опыту согласно пятифакторной модели личности. В результате работы был выделен ряд критериев для оценки степени открытости пользователя социальной сети, предложена модель, с помощью которой можно провести необходимый анализ. В дальнейшей работе планируется усовершенствовать математическую модель для получения более точной оценки: обучить модель на наборе данных вместо экспертной оценки условных вероятностей, а также добавить в модель не только численные характеристики, но и анализ контента, потребляемого и публикуемого пользователем в социальной сети.

Работа выполнена в рамках проекта по государственному заданию СПИИРАН № 0073-2019-0003, при финансовой поддержке РФФИ, проекты №20-07-00839.

СПИСОК ЛИТЕРАТУРЫ

- [1] Как обезопасить себя в соц. сетях. Рекомендации эксперта. URL: <https://www.m24.ru/news/obshchestvo/16072020/125353> (дата обращения: 20.09.2020)
- [2] Подходы к разработке моделей для анализа текстовой информации в профилях социальной сети в целях построения профиля

- уязвимостей пользователя. URL: <https://elibrary.ru/item.asp?id=29850652> (дата обращения: 20.09.2020)
- [3] Learning Bayesian Networks Neapolitan R.E., 2004
- [4] Тулупьев А. Л. Алгебраические байесовские сети: локальный логико-вероятностный вывод. - СПб ВВМ, 2019. С. 2-12
- [5] Щебетенко С. А. Большая пятерка черт личности и активность пользователей в социальной сети «ВКонтакте» - Вестник ЮУрГУ. Серия «Психология» №6, 2018. С. 73-83.
- [6] Khlobystova, A.O., Abramov, M.V., Tulupyyev, A.L., Zolotin, A.A. Search for the shortest trajectory of a social engineering attack between a pair of users in a graph with transition probabilities // Informatsionno-Upravliaushchie Sistemy. 2018. No. 6. Pp. 74-81
- [7] Abramov, M.V., Azarov, A.A. Identifying user's of social networks psychological features on the basis of their musical preferences // Proceedings of 2017 20th IEEE International Conference on Soft Computing and Measurements, SCM 2017. 2017. Pp. 90-92
- [8] E. D. Frauenstein, S. Flowerday Susceptibility to phishing on social network sites: A personality information processing model - Elsevier Ltd, 2017.
- [9] M. Gratian, S. Bandi, M. Cukier, J. Dykstra, A. Ginther Correlating Human Traits and Cybersecurity Behavior Intentions - Elsevier Ltd, 2017.
- [10] Калашников И. Д. Статистические модели для данных социальных сетей и использование байесовской методологии - Финансовый университет 2019. С 406-409.
- [11] Тропова А. В., Тулупьева Т. В. Байесовская сеть доверия как модель оценки интенсивности поведения пользователя на примере постинга в социальной сети - СПбГЭТУ ЛЭТИ 2020. С 20-22.
- [12] Тулупьев А. Л., Пашенко А. Е., Азаров А. А. Информационная модель пользователя, находящегося под угрозой соционинженерной атаки - СПИИРАН, 2010. С 143-155.
- [13] Абрамов М. В., Азаров А. А. Моделирование соционинженерных атак с использованием байесовских сетей доверия - СПбГЭТУ ЛЭТИ, 2016. С 71-74.
- [14] Youyou W., Kosinski M., Stillwell D. Computer-based personality judgments are more accurate than those made by humans // Proceedings of the National Academy of Sciences of the United States of America. 2015. Vol. 112 (4). Pp. 1036-1040.
- [15] C. Wolverton, D. Stevens The impact of personality in recognizing disinformation - University of Louisiana at Lafayette, Lafayette, Louisiana, USA. С 181-191.
- [16] Шаламов Р. А., Абрамов М. В., Тулупьева Т. В. Автоматизация оценки степени выраженности психологических особенностей пользователей в управлении кадрами: тестирование в социальной сети - Концерн ЦНИИ Электроприбор, 2018. С 497-500.
- [17] Абрамов М. В., Азаров А. А., Тулупьева Т. В., Тулупьев А. Л. Модель профиля компетенции злоумышленника в задаче анализа защищенности персонала информационных систем от соционинженерных атак - Информационно-управляющие системы 2016. С. 77-84.
- [18] Jan-Erik Lönnqvist, Juha V.A. Itkonen, Markku Verkasalo, Panu Poutvaara The Five-Factor Model of personality and Degree and Transitivity of Facebook social networks - Journal of Research in Personality, volume 50, June 2014. С 98-101.
- [19] Абрамов М. В., Азаров А. А. Выявление психологических особенностей пользователей социальных сетей на основании музыкальных предпочтений - СПбГЭТУ ЛЭТИ 2017. С 130-133.
- [20] Хромов А. Б. Пятифакторный опросник личности: Учебно-методическое пособие - КГУ, 2000. С 2-22.
- [21] Воронкова Я. Ю., Радюк О.М., Басинская И.В. "Большая пятерка" или пятифакторная модель личности - Тихоокеан. гор. ун-т, 2017. С 39-45.
- [22] Goldberg L. R. An alternative «description of personality»: The Big-Five factor structure - Journal of Personality and Social Psychology, 1990. Т. 59, № 6, С. 1216-1229.
- [23] Goldberg L. Language and individual differences: the search for universals in personality lexicons - Review of Personality and Social Psychology, 1981. Т. 2, С. 141-165.
- [24] Zhao H. The big five personality dimensions and entrepreneurial status: a meta-analytical review - The Journal of applied psychology, 2006. Т. 91, № 2, С. 259-71.
- [25] Бурлачук Л.Ф.- Словарь-справочник по психодиагностике, 2007. С 689-690..
- [26] Пятифакторный личностный опросник. URL: <http://www.syntone-spb.ru/library/news/content/283.html> (дата обращения: 08.12.2020)
- [27] Количество атак с использованием социальной инженерии выросло на 147% в 2020 году. URL: <https://www.securitylab.ru/news/515178.php> (дата обращения: 11.03.2021)
- [28] Степанова М. М., Хайкин В. Д.1 Анализ контента социальных сетей с целью диагностики психологического портрета личности - ООО "Консалтинговая компания Юком", 2012. С 136-137.
- [29] Zakieh S. E., Mohammad M. R. K., Farnaz J. M., Simin S., Zahra T., Shima M. E. & Koosha S. O. Bayesian network modeling for diagnosis of social anxiety using some cognitive-behavioral factors - Network

- [30] Hulya Olmus, S.Oral Erbas Determining the conditional probabilities in bayesian networks - Hacettepe Journal of Mathematics and Statistics volume33, 2004. С 69-76.
- [31] Азаров А.А., Тулупьева Т.В., Суворова А.В., Тулупьев А.Л., Абрамов М.В., Юсупов Р.М. Социоинженерные атаки. Проблемы анализа. — СПб.: Наука, 2016. С 352.
- [32] Станкевич М. А., Игнатьев Н. А., Смирнов И. В., Кисельникова Н. В. Выявление личностных черт у пользователей социальной сети ВКонтакте - Психологический институт РАО, 2019, №4. С 80-87..
- [33] Сапон И. В., Леденев Д. Е. Виртуальная личность: сетевой эффект самораскрытия - СибГУТИ, 2020. С 36-50.
- [34] Сапон И.В., Леденев Д.Е. Мотивы использования социальной сети как фактор самораскрытия в профиле - СибГУТИ, 2020. С 75-78.
- [35] Леденев Д. Е. Медиаактивность как фактор самораскрытия в профиле социальной сети - СибГУТИ, 2020. С 322-235.
- [36] Безбогова М. С., Ионцева М. В. Социально-психологические аспекты взаимодействия пользователей в виртуальных социальных сетях - ФГБОУ ВО ГУУ, 2016. С 43.
- [37] Злоказов К. В., Колмыкова Т. И., Рыбьякова В. А. Влияние экстраверсии, нейротизма и психотизма на восприятие информации об угрозе здоровью, репутации и социальному статусу - УрГПУ, Педагогическое образование в России, 5, 2017. С 75-83.
- [38] С. А. Щебетенко Установки на черты личности как предиктор активности “друзей” пользователя социальной сети “ВКонтакте” - Национальный психологический журнал. 2016. Т. 4. № 24. С. 34-44.
- [39] Cusack, B., & Adedokun, K. (2018). The impact of personality traits on user's susceptibility to social engineering attacks. DOI: <https://doi.org/10.25958/5c528ffa66693>