УНИВЕРСИТЕТ ИТМО
НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ
март–апрель 2018 Том 18 № 2 ISSN 2226-1494 http://ntv.ifmo.ru/
SCIENTIFIC AND TECHNICAL JOURNAL OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTICS
March–April 2018 Vol. 18 No 2 ISSN 2226-1494 http://ntv.ifmo.ru/en

УДК 004.056.53

ЗАДАЧИ АНАЛИЗА ЗАЩИЩЕННОСТИ ПОЛЬЗОВАТЕЛЕЙ ОТ СОЦИОИНЖЕНЕРНЫХ АТАК: ПОСТРОЕНИЕ СОЦИАЛЬНОГО ГРАФА ПО СВЕДЕНИЯМ ИЗ СОЦИАЛЬНЫХ СЕТЕЙ

М.В. Абрамов[a,b], А.Л. Тулупьев[a,b], А.А. Сулейманов[a,b]

[a] СПИИРАН, Санкт-Петербург, 199178, Российская Федерация
[b] Санкт-Петербургский государственный университет, Санкт-Петербург, 198504, Российская Федерация
Адрес для переписки: alexander.tulupyev@gmail.com

Информация о статье
Поступила в редакцию 25.01.18, принята к печати 28.02.18
doi: 10.17586/2226-1494-2018-18-2-313-321
Язык статьи – русский

Ссылка для цитирования: Абрамов М.В., Тулупьев А.Л., Сулейманов А.А. Задачи анализа защищенности пользователей от социоинженерных атак: построение социального графа по сведениям из социальных сетей // Научно-технический вестник информационных технологий, механики и оптики. 2018. Т. 18. № 2. С. 313–321. doi: 10.17586/2226-1494-2018-18-2-313-321

Аннотация

Предмет исследования. Аккаунты в социальных сетях как источник сведений об интенсивности общения между сотрудниками в коллективе (или группе), на основании которых строятся оценки вероятности успеха распространения социоинженерной атаки злоумышленника на пользователя. **Цель исследования.** Построить оценку успеха многоходовой социоинженерной атаки злоумышленника на пользователя, базирующуюся на сведениях, получаемых из аккаунтов сотрудников компании в социальных сетях и характеризующих интенсивность общения между ними. Исследование направлено на разработку моделей и алгоритмов распространения социоинженерной атаки на прореженном социальном графе компании и описание методов расчета оценок защищенности пользователей информационной системы от многоходовых социоинженерных атак, т.е. атак, где цель и точка входа не совпадают. **Метод.** Используются методы поиска, сопоставления и анализа сведений, характеризующих интенсивность общения между сотрудниками компании и извлекаемых из них аккаунтов в социальных сетях. Оценка вероятности успеха многоходовой социоинженерной атаки сводится к построению оценки вероятности сложного события. **Основные результаты.** Представлена формула для расчета оценок вероятностей распространения социоинженерной атаки между пользователями; полученные таким образом оценки сопоставляются дугам в социальном графе компании, используемом, в свою очередь, при оценке вероятности успеха многоходовой социоинженерной атаки, т.е. атаки, проходящей через цепочку пользователей. В более ранних исследованиях данные оценки вероятностей задавались экспертно. Описаны преимущества автоматизации расчета оценок вероятностей на основе данных, получаемых из социальных сетей. **Новизна исследования.** В исследовании рассматриваются подходы к оценке успеха многоходовых (опосредованных, не прямых, не сводящихся к одному непосредственному атакующему действию злоумышленника) социоинженерных атак на пользователя с учетом его связей в социальном графе, причем характеристики связей в графе строятся на основе данных, извлеченных из социальных сетей. **Практическая значимость.** Предложенный в работе подход создает основу для последующего анализа возможных траекторий распространения многоходовых социоинженерных атак, а также для расчета вероятностей реализации каждой такой траектории, что, в свою очередь, способствует расширению числа учитываемых факторов, влияющих на оценку защищенности пользователей информационной системы, и позволяет ставить задачу бэктрекинга атак в одной из удачных для поиска решений форм.

Ключевые слова
информационная безопасность, социоинженерные атаки, социотехнические атаки, защита пользователя, социальный граф пользователей, безопасность киберсоциальных систем

Благодарности
Работа выполнена в рамках проекта по государственному заданию СПИИРАН № 0073-2014- 0002, при финансовой поддержке РФФИ, проект №16-31- 00373 – Методы идентификации параметров социальных процессов по неполной информации на основе вероятностных графических моделей; проект №18-01- 00626 – Методы представления, синтеза оценок истинности и машинного обучения в алгебраических байесовских сетях и родственных моделях знаний с неопределенностью: логико-вероятностный подход и системы графов; проект № 18-37- 00323 – Социоинженерные атаки в корпоративных информационных системах: подходы, методы и алгоритмы выявления наиболее вероятных траекторий.

ANALYSIS OF USERS' PROTECTION FROM SOCIO-ENGINEERING ATTACKS: SOCIAL GRAPH CREATION BASED ON INFORMATION FROM SOCIAL NETWORK WEBSITES

M.V. Abramov[a, b], A.L. Tulupyev[a, b], A.A Suleymanov[a, b]

[a] SPIIRAS, Saint Petersburg, 199178, Russian Federation
[b] Saint Petersburg State University, Saint Petersburg, 198504, Russian Federation
Corresponding author: alexander.tulupyev@gmail.com

Article info
Received 25.01.18, accepted 28.02.18
doi: 10.17586/2226-1494-2018-18-2-313-321
Article in Russian
For citation: Abramov M.V., Tulupyev A.L., Suleymanov A.A. Analysis of users' protection from socio-engineering attacks: social graph creation based on information from social network websites. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2018, vol. 18, no. 2, pp. 313–321 (in Russian). doi: 10.17586/2226-1494-2018-18-2-313-321

Abstract

Subject of Research. The paper deals with accounts in social network websites as a source of information about the intensity of communication between employees in the team. On their basis we form success probability estimates for the spread of malefactor socio-engineering attack on the user. **Scope of Research.** The research goal is to build a success assessment for malefactor multi-pass socio-engineering attack on the user based on information obtained from the accounts of company employees in social network websites which characterizes communication intensity between them. The research is aimed at development of models and algorithms for socio-engineering attack spreading on the collapsed social graph of the company and description of methods for calculation of security estimates for the information system users from multi-pass socio-engineering attacks, such attacks, where the target and the entry point do not match. **Method.** The methods are used of information searching, comparing and analyzing, which characterizes communication intensity between company employees, and data extracted from their accounts in social network websites. Success probability estimate of multi-pass socio-engineering attack reduces to probability estimate creation of a complex event. **Main Results.** A formula is presented for calculating of probability estimates of socio-engineering attack propagation between users. The estimates obtained in this way are compared to the arcs in the company's social graph, which is used in turn to assess the success probability of a multi-pass socio-engineering attack, the attack, passing through a chain of users. In the earlier studies, estimates of probabilities were defined expertly. The advantages of calculation automating of probability estimates based on data received from social network websites are described. **Research Novelty.** The paper considers approaches to probabilistic estimates of multi-pass socio-engineering attack success where attacks are intermediate, non-direct, and non-reducible to a single malefactor act. These estimates take into account user's links in his or her social graph; the parameters of those links are based on the data obtained from social media/networks. **Practical Relevance.** The approach proposed in this paper provides the basis for further analysis of possible propagation trajectories of multi-pass social engineering attacks, as well as calculation of the probability of each such trajectory that in turn helps to expand the number of factors affecting the security evaluation of the information system users, and gives the possibility to set the backtracking task for attacks in one of the successful forms for finding solutions.

Keywords
information security, socio-engineering attacks, socio-technical attacks, user protection, social user graph, cybersocial system security

Acknowledgements
The research was carried out in the framework of the project on SPIIRAS state assignment No. 0073-2014-0002, with the financial support of the RFBR (project No. 16-31-00373 "Methods for parameters identifying of social processes from incomplete information based on probabilistic graphic models"; project No. 18-01-00626 "Methods of representation, synthesis of truth estimates and machine learning in algebraic Bayesian networks and related knowledge models with uncertainty: the logic-probability approach and graph systems"); project No. 18-37-00323 – Socio-engineering attacks in corporate information systems: approaches, methods and algorithms for identifying the most probable trajectories.

Введение

Хотя большая часть исследований и публикаций в сфере информационной безопасности относится к ее программно-техническим аспектам, проблемы, связанные с ее социотехническими (социоинженерными) аспектами, оказались не менее важны, поскольку пользователь информационной системы является ее наиболее уязвимым звеном [1–5]. Важность анализа информационной безопасности в срезе социоинженерных (социотехнических) атак также подтверждается большим количеством освещаемых в средствах массовой информации инцидентов, высокой востребованностью компаний, производящих соответствующее программное обеспечение, серийностью научных публикаций [6–12]. Отметим, что термины «социоинженерные атаки» и «социотехнические атаки» рассматриваются как синонимы. Наряду с этим б**о**льшая часть исследований в области информационной безопасности посвящена защите от программно-технических атак. В настоящее время отсутствуют стандартизованные методики оценки защищенности персонала информационной системы от социоинженерных атак, т.е. атак, которые, в частности, задействуют манипулятивные техники для воздействия на пользователя с целью достижения желаемого результата, например, нарушения конфиденциальности критичного документа [10]. При этом все острее ощущается необходимость анализа защищенности пользователей информационных систем от таких атак,

повышения на его основе уровня безопасности киберсоциальных систем, а также потребность в инструментах для профилактики, бэктрекинга, расследования и предотвращения соответствующих преступлений. Такие разработки позволили бы существенно сократить количество успешных социоинженерных инцидентов, что непосредственно повлияло бы на сокращение размера ущерба компаний. Таким образом, актуальной видится общая цель исследования, заключающаяся в формировании подходов, методов, алгоритмов, методик анализа и оценки защищенности пользователей от социоинженерных атак, а также в разработке систем упреждающей диагностики и бэктрекинга инцидентов [10].

Для достижения обозначенной общей цели исследования необходимо решить ряд частных задач, одна из которых рассматривается в данной работе. Ее материал посвящен решению задачи разработки моделей и алгоритмов распространения социоинженерной атаки на прореженном социальном графе компании [13] и описанию метода расчета оценок защищенности пользователей информационной системы от многоходовых социоинженерных атак (опосредованных атак, не прямых атак), т.е. атак, где цель и точка входа не совпадают. С точки зрения вычислений, цель состоит в разработке алгоритма расчета вероятностей (оценок вероятностей) успеха социоинженерных атак. Данный алгоритм агрегирует информацию, извлекаемую из социальной сети, о следующих параметрах: наличие пользователей друг у друга в семейном положении, в публичных списках друзей (лучшие друзья, родственники, коллеги и т.д.), наличие общих фотографий (определяется по отметкам), интенсивность взаимной активности на страницах друг друга, выраженной в отметках «Мне нравится» (иными словами, в лайках) и репостах, пересечение в подписках и друзьях. Отметим, что подходы к оценке успеха непосредственного атакующего действия злоумышленника-социоинженера на пользователя уже разрабатываются [10], однако и в них остаются открытые вопросы.

Релевантные исследования

В настоящее время растет число пользователей социальных сетей. При этом большинство из них не задумывается о соблюдении мер информационной безопасности, добровольно публикуя данные о себе [14]. Между тем доступ к этим данным может также получить злоумышленник, а следовательно, и учитывать их при планировании атаки. Такая информация имеет высокую ценность также потому, что выводы, основанные на публикуемом пользователем контенте в социальной сети, как правило, больше соответствуют действительности, чем получаемые в рамках опросов или интервью [7, 15].

Заделом для достижения цели настоящей работы служит то, что уже реализованы методы и алгоритмы, позволяющие автоматизировано осуществлять поиск аккаунтов сотрудников компании в социальной сети ВКонтакте (https://vk.com/) [16]. Согласно статистическим исследованиям, данная социальная сеть является одной из самых популярных на территории Российской Федерации [17]. Существуют методы выявления степени выраженности психологических особенностей, исходя из анализа контента, публикуемого на странице пользователя [15, 18–20]. Уже разработаны подходы к оценке вероятности успеха социоинженерного атакующего воздействия [21]. При этом зачастую атака происходит не непосредственно на пользователя, а через его коллег, и успех ее развития, как правило, зависит от характера взаимоотношений, интенсивности взаимодействия между сотрудниками в компании. Таким образом, для оценки вероятности успеха прохождения социоинженерной атаки через сотрудников компании необходимо определить интенсивность их взаимодействия. Это можно сделать разными способами, например, прибегнув к экспертным оценкам. В данной работе впервые предлагается подход к оценке вероятности прохождения атаки между сотрудниками, основанный на интенсивности взаимодействия между ними, определяемой через анализ аккаунтов в социальных сетях. Также впервые предлагается подход к оценке успешности многоходовой атаки злоумышленника на пользователя информационной системы компании, т.е. атаки, цель которой не совпадает с первым атакуемым пользователем.

Подход к построению и анализу социального графа сотрудников компании

Предполагается, что чем многочисленнее связи между пользователями информационной системы, тем большее число способов потенциально доступно злоумышленнику для реализации атаки. Представляется весьма правдоподобным предположение, что чем больше количество и интенсивность связей между двумя сотрудниками, тем с большей вероятностью злоумышленник сможет развить социоинженерную атаку, переходя от одного из них к другому.

Для оценки вероятностей успеха распространения сложной социоинженерной атаки предлагается построить социальный граф сотрудников компании. В социальном графе множество вершин сопоставлено множеству сотрудников компании, а множество ребер – связями между ними. Отметим, что в общем случае в начале нашего построения данный граф будет являться полным, поскольку каждая пара вершин будет смежной, и неориентированным. Его ребрам сопоставлены оценки вероятностей, которые отражают характер взаимоотношений между сотрудниками (метод расчета этих оценок описан ниже). Обработка полного графа является довольно проблематичной в реализации задач аналитического моделирования даже для относительно небольшого числа сотрудников. Хранение и обработка такого графа требует

больших затрат памяти и лишней работы процессора. Для иллюстрации этого факта возьмем среднюю компанию с численностью сотрудников 100 человек. Получим следующие показатели для числа ребер и опосредованных атак, состоящих из цепочек, включающих трех сотрудников:

$$K_{100} = \frac{100(100-1)}{2} = 4950;$$

$$A_{100}^3 = 100 \cdot 99 \cdot 98 = 970200,$$

где K_{100} – число ребер в социальном графе, состоящем из 100 сотрудников, а A_{100}^3 – число цепочек, включающих трех сотрудников. Таким образом, для достижения приемлемой сложности вычислений потребуется «проредить» полный граф.

Можно говорить о трех ключевых подходах к обработке и анализу получаемого социального графа:

1. анализ полного графа – как контрольный образец (иными словами, «золотой стандарт» – теоретически идеальный, но дорогостоящий, и в реальных задачах вычислительно недостижимый), используемый для сравнения с результатами анализа, полученными в соответствии с другими подходами;
2. использование ограничений, связанных с устройством, организацией деятельности компании – как часто применяемый ограничитель, имеющий свои плюсы и минусы. В этом случае ребра исключаются на основании экспертных оценок;
3. использование пороговых значений – наиболее универсальный и допускающий автоматизацию способ, когда устанавливается минимальное значение для оценок вероятностей, а ребра с оценками, меньше этого значения, исключаются из рассмотрения.

Два последних подхода как раз позволяют вести вычисления на графе, более разреженном, чем полный социальный граф. В разрабатываемом алгоритме используется третий из приведенных выше подходов, который позволяет при расчетах существенно сократить число ребер, как предполагается, без существенной потери точности оценки вероятности успеха социоинженерной атаки, в силу того, что из рассмотрения исключаются малые вероятности, оказавшиеся ниже заданного порога. Компромиссы в отношении точности и скорости вычислений такого рода дискутировались в [22].

Расчет оценок вероятностей успеха распространения социоинженерной атаки на социальном графе

Согласно формуле, выведенной ранее [10], вероятность успеха социоинженерной атаки злоумышленника в социальном графе от пользователя m до пользователя j через пользователей i_k рассчитывается как

$$\tilde{P}_{m-\ldots-i_k-\ldots-j} = P_m \prod_{k=1}^{n-1} \tilde{P}_{i_k,i_{k+1}},$$

где $i_1 = m, i_n = j$, P_i – вероятность успешности атаки на i-го сотрудника, если у злоумышленника есть на него выход, $\tilde{P}_{i_k,i_{k+1}}$ – вероятность выхода злоумышленника на пользователя i_{k+1} через пользователя i_k, если пользователь i_k уже успешно атакован. При этом вероятности успешности атаки на пользователя через другого пользователя в работе [10] задавались экспертно на основании характера их взаимоотношений. Такой подход является затруднительным для крупных компаний, где работает существенное количество сотрудников. Даже для относительно небольших компаний, например, состоящих из 15 человек, необходимо будет оценить вероятности перехода по 105 связям. При этом отметим, что отношения между сотрудниками в коллективе могут меняться с течением времени, что будет приводить к необходимости корректировки значений оцениваемых параметров. Таким образом, автоматизация процесса сопоставления дугам графа социальных связей оценок вероятностей успеха прохождения социоинженерной атаки через них позволит, в конце концов, сэкономить время на анализе степени защищенности, сделать его более оперативным. Предлагается подход к расчету этих оценок вероятностей, основанный, в свою очередь, на оценке вероятности перехода по данной дуге, причем эта оценка строится на основе сведений об интенсивности общения между соответствующей парой сотрудников. Оценки вероятности предполагается рассчитывать, исходя из общедоступных данных, публикуемых в социальных сетях.

Пусть p_{rel} – вероятность успеха распространения атаки от сотрудника к сотруднику, основанная на типе декларируемой в социальной сети связи. Тогда

$$p_{\text{rel}} = \begin{cases} p_0, \text{ (0) если пользователи отметили друг друга в графе семейное положение;} \\ p_1, \text{ (1) если пользователи находятся в публичных списках лучших друзей, но не (0);} \\ p_2, \text{ (2) если пользователи находятся в друзьях, но не (1);} \\ p_3, \text{ (3) если кто-то из пользователей подписан на другого, но не (2);} \\ p_4, \text{ (4) ничего из выше перечисленного.} \end{cases}$$

Также отметим, что $p_0 > ... > p_4$. Введем оценки вероятностей $p_{\text{likes}}, p_{\text{reposts}}, p_{\text{com\_photos}}, p_{\text{com\_groups}}$, характеризующие соответственно вклад отдельного эпизода каждого типа связи в оценку вероятности успеха распространения атаки от сотрудника к сотруднику. Кумулятивный вклад каждого типа связи тогда рассчитывается на основании числа лайков, репостов, общих фотографий и сообществ. При таких предположениях вероятности того, что социоинженерная атака не завершится успехом при одном эпизоде определенного типа связи, соответственно будут равны

$1 - p_{\text{rel}}; 1 - p_{\text{likes}}; 1 - p_{\text{reposts}}; 1 - p_{\text{com\_photos}}; 1 - p_{\text{com\_groups}}$.

Теперь требуется построить модель так, чтобы каждый эпизод в зависимости от типа связи вносил свой вклад в снижение оценки степени защищенности (если сформулировать строже – ожидаемого значения оценки степени защищенности).

Для расчета оценки вероятности того, что социоинженерная атака не распространится между пользователями, предлагается адаптировать модель Белла–Тревино [23], т.е., по существу, свести решение стоящей задачи к биоинспирированным вычислениям (biologically inspired computations) [24]. Модель Белла–Тревино (более точно – серия моделей, в построении и исследовании которых принимали участие эти исследователи) увязывает оценку риска с числом эпизодов рискованного поведения. В нашем случае в качестве числа эпизодов (в данном контексте это число – характеристика интенсивности связи) будут выступать количественные показатели, извлекаемые из аккаунтов в социальных сетях (число лайков, репостов, совместных фотографий, общих сообществ). Таким образом, оценка вероятности того, что социоинженерная атака не распространится между пользователями, с учетом интенсивности различных видов связи будет рассчитываться по формуле

$$Q = (1 - p_{\text{rel}})(1 - p_{\text{likes}})^{\text{count\_likes}}(1 - p_{\text{reposts}})^{\text{count\_reposts}}(1 - p_{\text{com\_photos}})^{\text{count\_photos}}(1 - p_{\text{com\_groups}})^{\text{count\_groups}}, \quad (1)$$

где 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. Вероятности того, что социоинженерная атака распространится между пользователями, с учетом интенсивности различных видов связи будет рассчитываться как вероятность дополнения указанного выше события «атака не распространится»:

$$P = 1 - Q. \quad (2)$$

Таким образом, алгоритм расчета оценок вероятностей успеха социоинженерных атак сводится к сбору информации из социальных сетей о связях пользователей [16], построению возможных, с точки зрения накопленной информации, деревьев атак [10] и агрегации полученной информации с помощью формул (1) и (2).

Численный пример. Методика оценки параметров $p_0, ..., p_4, p_{\text{likes}}, p_{\text{reposts}}, p_{\text{com\_photos}}, p_{\text{com\_groups}}$ разрабатывается особо, более того, такие методики, неизбежно учитывающие широкий спектр сведений от экспертов, информационных источников, в том числе из систем, обрабатывающих big data, поддержанные или реализованные в интеллектуальных (когнитивных) системах, могут оказаться проприетарными, входящими в систему знаний организации, которые позволяют ей конкурировать на рынке [25]. В иллюстративном вычислительном примере рассмотрим следующий набор значений:

$p_0 = 0,9,$ $p_3 = 0,3,$ $p_{\text{reposts}} = 0,4,$

$p_1 = 0,8,$ $p_4 = 0,1,$ $p_{\text{com\_photos}} = 0,6,$

$p_2 = 0,6,$ $p_{\text{likes}} = 0,2,$ $p_{\text{com\_groups}} = 0,3.$

Таким образом, в качестве примера посчитаем значение оценки вероятности успеха прохождения атаки на одного пользователя через другого при следующих исходных данных. Пусть

- два пользователя состоят друг у друга в списках друзей, но не отмечены в семейном положении и публичных списках лучших друзей;
- каждый поставил другому по три лайка;
- один из них сделал три репоста, а второй – два репоста постов другого;
- имеют три совместные фотографии;
- имеют пять общих подписок на сообщества.

В этом случае оценка вероятности успешного прохождения атаки на одного пользователя через другого будет рассчитываться следующим образом:

$$P_{i,i+1} = 1 - (1 - p_{\text{rel}})(1 - p_{\text{likes}})^{\text{count\_likes}}(1 - p_{\text{reposts}})^{\text{count\_reposts}}(1 - p_{\text{com\_photos}})^{\text{count\_photos}}(1 - p_{\text{com\_groups}})^{\text{count\_groups}} =$$

$$= 1 - (1 - 0,6)(1 - 0,2)^6(1 - 0,4)^5(1 - 0,6)^3(1 - 0,3)^5 \approx 0,99.$$

Описанным выше образом предлагается рассчитывать оценки вероятностей успеха прохождения атаки на сотрудника через другого сотрудника для всех пар сотрудников компании. Данные вероятности

будут, в свою очередь, использоваться для расчета оценок вероятности успеха многоходовой социоинженерной атаки на l-го пользователя через m-го по следующей формуле: $P_{ml} = P_l \prod_{i=m}^{l-1} P_{i,i+1}$, где P_i – вероятность успеха неопосредованной атаки злоумышленника на i-го пользователя, а $P_{i,i+1}$ – соответствующая оценка вероятности распространения атаки на пользователя через другого пользователя. Вместе с тем оценка защищенности пользователей информационной системы от социоинженерной атаки следующая: $P = 1 - P_{ml}$.

Обобщая изложенное, формула для расчета оценок вероятностей распространения социоинженерной атаки между двумя пользователями будет иметь следующий вид:

$$P_{i,i+1} = 1 - \prod_t \left(1 - p_t^{i,i+1}\right)^{n_t},$$

где $p_t^{i,i+1}$ – вероятность успеха социоинженерной атаки злоумышленника на пользователя по t-ой связи, n_t – число эпизодов, $P_{i,i+1}$ – оценка вероятности успеха распространения атаки на пользователя $i+1$ через пользователя i.

Пример построения социального графа

Представленная модель реализована в программном модуле для автоматизированного расчета оценок вероятности успеха перехода от пользователя к другому пользователю. Программный модуль строит социальный граф компании, помечая на дугах рассчитанные оценки. На рис. 1 представлен скриншот результатов работы данного модуля для небольшой компании, состоящей из 10 человек. В вершинах обозначены оценки вероятности успеха прямой атаки злоумышленника-социоинженера на пользователя. Так, например, оценка вероятности успеха социоинженерной атаки на пользователя Four через пользователей One, Two и Three будет рассчитываться по формуле

$$P_{1,2,3,4} = P_1 P_{1,2} P_{2,3} P_{3,4} = 0,8 \cdot 0,9 \cdot 0,94 \cdot 0,94 \approx 0,64.$$

Также существуют другие траектории в социальном графе сотрудников компании, по которым может распространяться социоинженерная атака на пользователя Four через пользователя One. Для иллюстративных целей допустим, что по результатам учета ряда факторов оказались приняты в рассмотрение три возможные траектории социоинженерной атаки на пользователя Four через пользователя One: One, Two, Three, Four; One, Two, Four; One, Three, Four. (Вопросы генерации деревьев атак и отбора траекторий атак обсуждались в [10].) Оценка вероятности распространения атаки по первой траектории представлена выше, по двум другим она будем рассчитываться следующим образом:

$$P_{1,2,4} = P_1 P_{1,2} P_{2,4} = 0,8 \cdot 0,9 \cdot 0,6 \approx 0,43; \quad P_{1,3,4} = P_1 P_{1,3} P_{3,4} = 0,8 \cdot 0,94 \cdot 0,94 \approx 0,7.$$

В таком случае оценка вероятности того, что злоумышленник-социоинженер не сможет успешно атаковать пользователя будет следующей:

$$Q = (1 - P_{1,2,3,4})(1 - P_{1,2,4})(1 - P_{1,3,4}) \approx 0,19,$$

а вероятность успеха атаки составит $P = 1 - Q \approx 0,81$.

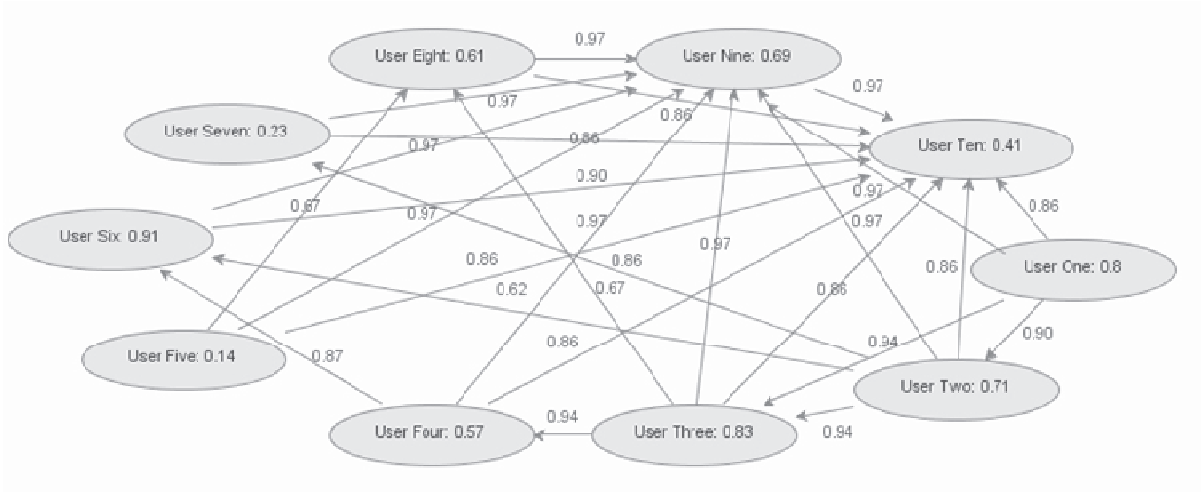

Рис. 1. Пример социального графа для компании, состоящей из 10 человек

Место в общей архитектуре комплекса

На основании представленных результатов построены алгоритмы построениея оценок на дугах и расчета оценки вероятности атаки, реализованные в модуле «Анализатор атак» разрабатываемого комплекса программ для оценки степени защищенности пользователей от социоинженерных атак (отметим, что в перспективе этот комплекс будет использован как система упреждающей диагностики и бэктрекинга инцидентов). Диаграмма основных модулей комплекса программ приведена на рис. 2. Модуль «Анализатор атак» в качестве входных данных посредством API получает JSON-файл, содержащий аккаунты сотрудников компании в социальной сети ВКонтакте, а на выходе передает JSON-файл с размеченными ребрами. JSON-файл, содержащий аккаунты сотрудников компании в социальной сети ВКонтакте, формируется модулем «Поиск персонала», методы, модели и алгоритмы для работы которого описаны в [16].

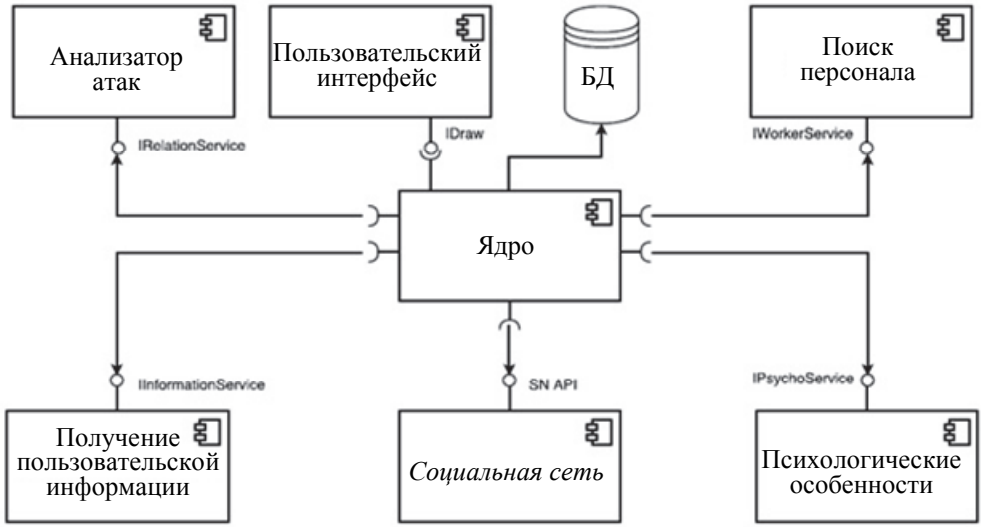

Рис. 2. Диаграмма компонент комплекса программ для оценки защищенности персонала информационной системы (БД – база данных)

Заключение

В работе предложены решение задачи расчета оценок вероятностей успеха прохождения социоинженерной атаки между пользователями на ребрах социального графа компании, а также вывод оценок вероятности успеха многоходовой социоинженерной атаки злоумышленника на пользователя. Приведенный алгоритм создает основу для последующего анализа возможных траекторий распространения этих атак, что способствует построению более точных оценок защищенности пользователей информационной системы за счет агрегации расширенного набора параметров, влияющих на оценку. Полученные в данной работе результаты обеспечивают агрегирование доступных из социальных сетей сведений о характере взаимоотношений между сотрудниками компании.

Предложенные решения отличаются тем, что оценка успеха производится в отношении многоходовой социоинженерной атаки, в которую вовлекаются несколько человек, а не в отношении единичного непосредственного атакующего действия социоинженера, направленного на пользователя, являющегося целью. Иными словами, рассматриваются атаки, точка входа и цель которого не совпадают. Кроме того, характеристики связей в социальном графе, который используется при расчете оценок успеха атаки, строятся на основе данных, извлеченных из социальных сетей.

Одним из направлений дальнейших исследований является разработка методик оценки параметров, характеризующих влияние отдельных показателей на определение значения оценки вероятности. Предполагается, что методики могут опираться на экспертный подход, результаты полевых социально-психологических исследований или на комбинацию этих двух подходов. Также планируется обеспечить агрегирование информации не только из социальной сети ВКонтакте, но и из других социальных сетей, а вместе с тем расширять число агрегируемых параметров для построения оценок.

Наконец, с точки зрения разработки программ превентивных вмешательств, нацеленных на предотвращение инцидентов в сфере информационной безопасности, связанных с социоинженерными атаками, учитывая то, что на тесноту/разреженность сложившихся в коллективе компании связей влиять затруднительно или бесполезно, можно пытаться уменьшить вероятность успешного использования злоумышленником той или иной связи между сотрудниками. Для этого необходимо разработать комплекс профилактических мер, среди которых могут быть такие, как проведение соответствующих тренингов, ограничения (либо оптимизации распределения) прав доступа к критичным документам, перепланировки офисно-

го пространства, а также изучить эффект от таких мер на изменение степени защищенности пользователей от социоинженерных атак.

Литература

1. Liu J., Lyu Q., Wang Q., Yu X. A digital memories based user authentication scheme with privacy preservation // PloS ONE. 2017. V. 12. N 11. Art. e0186925. doi: 10.1371/journal.pone.0186925
2. van Schaik P., Jeske D., Onibokun J., Coventry L., Jansen J., Kusev P. Risk perceptions of cyber-security and precautionary behaviour // Computers in Human Behavior. 2017. V. 75. P. 547–559.
3. The Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within [Электронный ресурс]. Kaspersky Lab. 2017. URL: https://www.kaspersky.com/blog/the-human-factor-in-it-security/ (дата обращения: 06.10.2017)
4. Аношин И. Карточные слабости. Как не стать жертвой высокотехнологичных мошенников // РБК. Газета. 2017. № 164. URL: http://www.rbc.ru/newspaper/2017/09/29/59ca447b9a79474aa6f65673 (дата обращения: 06.10.2017)
5. Antonyuk E.M., Varshavsky I.E., Antonyuk P.E. Adaptive systems of automatic control with prioritized channels // Proc. 20th IEEE Int. Conf. on Soft Computing and Measurements. St. Petersburg, 2017. P. 539–540. doi: 10.1109/SCM.2017.7970643
6. Desnitsky V.A., Kotenko I.V. Modeling and analysis of security incidents for mobile communication mesh Zigbee-based network // Proc. 20th IEEE Int. Conf. on Soft Computing and Measurements. St. Petersburg, 2017. P. 500–502. doi: 10.1109/SCM.2017.7970629
7. Du J., Jiang C., Chen K.C., Ren Y., Poor H.V. Community-structured evolutionary game for privacy protection in social networks // IEEE Transactions on Information Forensics and Security. 2018. V. 13. N 3. P. 574–589. doi: 10.1109/TIFS.2017.2758756
8. Gupta B.B., Tewari A., Jain A.K., Agrawal D.P. Fighting against phishing attacks: state of the art and future challenges // Neural Computing and Applications. 2017. V. 28. N 12. P. 3629–3654. doi: 10.1007/s00521-016-2275-y
9. Kotenko I., Chechulin A., Branitskiy A. Generation of source data for experiments with network attack detection software // Journal of Physics: Conference Series. 2017. V. 820. N 1. Art. 012033. doi: 10.1088/1742-6596/820/1/012033
10. 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. 352 с.
11. Митник К.Д., Саймон В.Л. Искусство обмана. М.: Компания АйТи, 2004. 416 с.
12. Ding D., Han Q.L., Xiang Y., Ge X., Zhang X.M. A survey on security control and attack detection for industrial cyber-physical systems // Neurocomputing. 2018. V. 275. P. 1674–1683. doi: 10.1016/j.neucom.2017.10.009
13. Corbellini A., Godoy D., Mateos C., Schiaffino S., Zunino A. DPM: A novel distributed large-scale social graph processing framework for link prediction algorithms // Future Generation Computer Systems. 2017. V. 78. P. 474–480. doi: 10.1016/j.future.2017.02.025
14. Su S., Li X., Cheng X., Sun C. Location-aware targeted influence maximization in social networks // Journal of the Association for Information Science and Technology. 2018. V. 69. N 2. P. 229–241.
15. Суворова А.В., Тулупьева Т.В., Тулупьев А.Л., Сироткин А.В., Пащенко А.Е. Вероятностные графические модели социально-значимого поведения индивида, учитывающие неполноту информации // Труды СПИИРАН. 2012. Т. 3. № 22. С. 101–112.
16. Shindarev N., Bagretsov G., Abramov M., Tulupyeva T., Suvorova A. Approach to identifying of employees profiles in websites of social networks aimed to analyze social engineering vulnerabilities // Advances in Intelligent Systems and Computing. 2017. V. 679. P. 441–447. doi: 10.1007/978-3-319-68321-8_45

References

1. Liu J., Lyu Q., Wang Q., Yu X. A digital memories based user authentication scheme with privacy preservation. *PloS ONE*, 2017, vol. 12, no. 11, art. e0186925. doi: 10.1371/journal.pone.0186925
2. van Schaik P., Jeske D., Onibokun J., Coventry L., Jansen J., Kusev P. Risk perceptions of cyber-security and precautionary behavior. *Computers in Human Behavior*, 2017, vol. 75, pp. 547–559.
3. The Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within. Kaspersky Lab. 2017. URL: https://www.kaspersky.com/blog/the-human-factor-in-it-security/ (accessed: 06.10.2017)
4. Anoshin I. Card weaknesses. How not to become a victim of high-tech scammers. *RBK, Newspaper*, 2017, no. 164. URL: http://www.rbc.ru/newspaper/2017/09/29/59ca447b9a79474aa6f65673 (accessed: 06.10.2017)
5. Antonyuk E.M., Varshavsky I.E., Antonyuk P.E. Adaptive systems of automatic control with prioritized channels. *Proc. 20th IEEE Int. Conf. on Soft Computing and Measurements*. St. Petersburg, 2017, pp. 539–540. doi: 10.1109/SCM.2017.7970643
6. Desnitsky V.A., Kotenko I.V. Modeling and analysis of security incidents for mobile communication mesh Zigbee-based network. *Proc. 20th IEEE Int. Conf. on Soft Computing and Measurements*. St. Petersburg, 2017, pp. 500–502. doi: 10.1109/SCM.2017.7970629
7. Du J., Jiang C., Chen K.C., Ren Y., Poor H.V. Community-structured evolutionary game for privacy protection in social networks. *IEEE Transactions on Information Forensics and Security*, 2018, vol. 13, no. 3, pp. 574–589. doi: 10.1109/TIFS.2017.2758756
8. Gupta B.B., Tewari A., Jain A.K., Agrawal D.P. Fighting against phishing attacks: state of the art and future challenges. *Neural Computing and Applications*, 2017, vol. 28, no. 12, pp. 3629–3654. doi: 10.1007/s00521-016-2275-y
9. Kotenko I., Chechulin A., Branitskiy A. Generation of source data for experiments with network attack detection software. *Journal of Physics: Conference Series*, 2017, vol. 820, no. 1, art. 012033. doi: 10.1088/1742-6596/820/1/012033
10. Azarov A.A., Tulup'eva T.V., Suvorova A.V., Tulup'ev A.L., Abramov M.V., Yusupov R.M. *Socio-Engineering Attacks: Problems of Analysis*. St. Petersburg, Nauka Publ., 2016, 352 p. (in Russian)
11. Mitnik K.D., Saimon V.L. *Art of Deceit*. Moscow, IT Company Publ., 2004, 416 p. (in Russian)
12. Ding D., Han Q.L., Xiang Y., Ge X., Zhang X.M. A survey on security control and attack detection for industrial cyber-physical systems. *Neurocomputing*, 2018, vol. 275, pp. 1674–1683. doi: 10.1016/j.neucom.2017.10.009
13. Corbellini A., Godoy D., Mateos C., Schiaffino S., Zunino A. DPM: A novel distributed large-scale social graph processing framework for link prediction algorithms. *Future Generation Computer Systems*, 2017, vol. 78, pp. 474–480. doi: 10.1016/j.future.2017.02.025
14. Su S., Li X., Cheng X., Sun C. Location-aware targeted influence maximization in social networks. *Journal of the Association for Information Science and Technology*, 2018, vol. 69, no. 2, pp. 229–241.
15. Suvorova A.V., Tulup'eva T.V., Tulup'ev A.L., Sirotkin A.V., Pashchenko A.E. Probabilistic graphical models of individual socially significant behavior on the base of incomplete data. *SPIIRAS Proceedings*, 2012, vol. 3, no. 22, pp. 101–112. (in Russian)
16. Shindarev N., Bagretsov G., Abramov M., Tulupyeva T., Suvorova A. Approach to identifying of employees profiles in websites of social networks aimed to analyze social engineering vulnerabilities. *Advances in Intelligent Systems and Computing*, 2017, vol. 679, pp. 441–447. doi: 10.1007/978-3-319-68321-8_45
17. *Social Networks in Russia*. Mail.Ru Group 2014. URL:

17. Социальные сети в России [Электронный ресурс]. Mail.Ru Group 2014. URL: https://corp.imgsmail.ru/media/files/issledovanie-auditorij-sotcialnykh-setej.pdf (дата обращения: 20.01.2018).
18. Bagretsov G.I., Shindarev N.A., Abramov M.V., Tulupyeva T.V. Approaches to development of models for text analysis of information in social network profiles in order to evaluate user's vulnerabilities profile // Proc. 20th IEEE Int. Conf. on Soft Computing and Measurements. St. Petersburg, 2017. P. 93–95.
19. Мальчевская Е.А., Бирилло А.И., Харитонов Н.А., Золотин А.А. Развитие матрично-векторного подхода в алгоритмах локального априорного вывода в алгебраических байесовских сетях // Труды VII Всероссийской научно-практической конференции «Нечеткие системы, мягкие вычисления и интеллектуальные технологии». Санкт-Петербург, 2017. Т. 1. С. 92–100.
20. Тулупьева Т.В. Тулупьев А.Л., Пащенко А.Е., Азаров А.А., Степашкин М.В. Социально-психологические факторы, влияющие на степень уязвимости пользователей автоматизированных информационных систем с точки зрения социоинженерных атак // Труды СПИИРАН. 2010. Т. 1. № 12. С. 200–214.
21. Абрамов М.В., Азаров А.А., Тулупьева Т.В., Тулупьев А.Л. Модель профиля компетенций злоумышленника в задаче анализа защищенности персонала информационных систем от социоинженерных атак // Информационно-управляющие системы. 2016. Т. 83. № 4. С. 77–84. doi: 10.15217/issn1684-8853.2016.4.77
22. Baccelli F., Chatterjee A., Vishwanath S. Pairwise stochastic bounded confidence opinion dynamics: heavy tails and stability // IEEE Transactions on Automatic Control. 2017. V. 62. N 11. P. 5678–5693. doi: 10.1109/TAC.2017.2691312
23. Bell D.C., Trevino R.A. Modeling HIV risk // Journal of Acquired Immune Deficiency Syndromes and Human Retrovirology. 1999. V. 22. N 3. P. 280–287.
24. Samsonovich A.V. On a roadmap for the BICA challenge // Biologically Inspired Cognitive Architectures. 2012. V. 1. P. 100–107. doi: 10.1016/j.bica.2012.05.002
25. Ginni Rometty on the End of Programming [Электронный ресурс]. Bloomberg. 2017. URL: https://www.bloomberg.com/news/features/2017-09-20/ginni-rometty-on-artificial-intelligence (дата обращения: 06.10.2017)

Авторы

Абрамов Максим Викторович – младший научный сотрудник, СПИИРАН, Санкт-Петербург, 199178, Российская Федерация; старший преподаватель, Санкт-Петербургский государственный университет, Санкт-Петербург, 198504, Российская Федерация, Scopus ID: 56938320500, ORCID ID: 0000-0002-5476-3025, mva16@list.ru

Тулупьев Александр Львович – доктор физико-математических наук, доцент, заведующий лабораторией, СПИИРАН, Санкт-Петербург, 199178, Российская Федерация; профессор, Санкт-Петербургский государственный университет, Санкт-Петербург, 198504, Российская Федерация, Scopus ID: 13608565400, ORCID ID: 0000-0003-1814-4646, alexander.tulupyev@gmail.com

Сулейманов Алексей Александрович – стажер, СПИИРАН, Санкт-Петербург, 199178, Российская Федерация; студент, Санкт-Петербургский государственный университет, Санкт-Петербург, 198504, Российская Федерация, ORCID ID: 0000-0002-9146-6249, lex.suleimanov@gmail.com

Authors

Maxim V. Abramov – Junior scientific researcher, SPIIRAS, Saint Petersburg, 199178, Russian Federation; Senior lecturer, Saint Petersburg State University, Saint Petersburg, 198504, Russian Federation, Scopus ID: 56938320500, ORCID ID: 0000-0002-5476-3025, mva16@list.ru

Alexander L. Tulupyev – D.Sc., Associate Professor, Head of laboratory, SPIIRAS, Saint Petersburg, 199178, Russian Federation; Professor, Saint Petersburg State University, Saint Petersburg, 198504, Russian Federation, Scopus ID: 13608565400, ORCID ID: 0000-0003-1814-4646, alexander.tulupyev@gmail.com

Alexey A. Suleymanov – trainee, SPIIRAS, Saint Petersburg, 199178, Russian Federation; student, Saint Petersburg State University, Saint Petersburg, 198504, Russian Federation, ORCID ID: 0000-0002-9146-6249, lex.suleimanov@gmail.com