Компьютерные инструменты в образовании, 2021
№ 3: 17–28
УДК: 004.056
http://cte.eltech.ru
doi:10.32603/2071-2340-2021-3-17-28

КОНЦЕПТУАЛЬНАЯ МОДЕЛЬ ЦИКЛА СОЦИОИНЖЕНЕРНОЙ АТАКИ: СОВРЕМЕННЫЕ ПОДХОДЫ И АРХИТЕКТУРА ПРОТОТИПА ПРОГРАММНОГО КОМПЛЕКСА*

Хлобыстова А. О.[1], младший научный сотрудник, ✉ aok@dscs.pro

[1]Санкт-Петербургский Федеральный исследовательский центр Российской академии наук (СПб ФИЦ РАН), 14 линия, 39, 199178, Санкт-Петербург, Россия

Аннотация

Социоинженерные атаки являются одной из ключевых проблем современности. С каждым годом их количество и эффективность сохраняют тенденцию роста. В настоящей работе приводится обзор существующих исследований, посвящённых проблеме защищенности пользователей от социоинженерных атак. На основе сделанного обзора предлагается концептуальная модель цикла социоинженерной атаки и архитектура прототипа программного комплекса, преимуществом которого перед существующими аналогами является учёт профиля злоумышленника и набор существующих инструментов для атаки. Практическая значимость заключается в создании основы для разработки программного решения для моделирования социоинженерной атаки и последующего выявления наиболее уязвимых сотрудников организации к социоинженерным атакам, учитывающее сведения о потенциальном объекте атаки.

Ключевые слова: *социоинженерные атаки, модель цикла социоинженерной атаки, профиль уязвимостей пользователя, модель злоумышленника.*

Цитирование: Хлобыстова А. О. Концептуальная модель цикла социоинженерной атаки: современные подходы и архитектура прототипа программного комплекса // Компьютерные инструменты в образовании. 2021. № 3. С. 17–28. doi: 10.32603/2071-2340-2021-3-17-28

1. ВВЕДЕНИЕ

В настоящее время отмечается заметный рост числа кибератак и их эффективности [1–4]. Согласно данным ФБР [1], в 2021 году число жалоб на цифровые преступления увеличилось примерно на 70 % по сравнению с 2019 и 2020 годами. При этом большинство таких жалоб связаны с социоинженерными атаками [1]. Под социоинженерной атакой понимается набор прикладных психологических и аналитических приемов, которые злоумышленники применяют для скрытой мотивации пользователей публичной или корпоративной сети к нарушениям устоявшихся правил и политик в области информационной безопасности [5]. Согласно данным компании Barracuda Network, занимающейся обеспечением информационной безопасности компаний, в среднем

* Работа выполнена в рамках проекта по государственному заданию СПб ФИЦ РАН СПИИРАН № 0073-2019-0003, при финансовой поддержке РФФИ, проект № 20-07-00839.

организации ежегодно подвергаются около 700 социоинженерным атакам [6]. Ухудшающаяся статистика социоинженерных инцидентов показывает, что существующие сегодня решения в области защиты пользователей информационных систем от социоинженерных атак оказываются недостаточно эффективными. То есть актуальна проблема разработки инструментов, способствующих повышению уровня защищённости пользователей от социоинженерных атак.

Целью настоящей работы является анализ современного состояния работ, посвящённых проблематике социоинженерных атак и построение на его основе концептуальной модели цикла социоинженерной атаки, а также предложение архитектуры прототипа программного комплекса, преимуществом которого перед существующими является учёт профиля злоумышленника и набора существующих инструментов для атаки. Практическая значимость заключается в создании основы для разработки программного решения для моделирования социоинженерной атаки и последующего выявления наиболее уязвимых сотрудников организации к социоинженерным атакам, учитывающее сведения о потенциальном объекте атаки.

2. СУЩЕСТВУЮЩИЕ ИССЛЕДОВАНИЯ

Рассмотрим исследования, посвященные проблематике социоинженерных атак, структурировав их следующим образом: исследования, описывающие факторы, влияющие на успех социоинженерной атаки, модели цикла социоинженерной атаки, подходы и решения по анализу защищённости от социоинженерных атак и анализ информации из открытых источников в контексте социоинженерных атак.

2.1. Исследования, описывающие факторы, влияющие на успех социоинженерной атаки

На первом этапе важно оценить степень защищенности пользователей информационной системы от социоинженерных атак. Для формализации этой оценки необходимо изучить факторы, влияющие на успех социоинженерной атаки. Для выделения этих факторов, в свою очередь, предлагается рассмотреть социоинженерные инциденты. Информация о таких инцидентах находит отражение в научной, научно-популярной и иной литературе [3, 4, 6–13]. В [14] представлены результаты анализа интервью с 37 злоумышленниками-социоинженерами. Респонденты были набраны через различные съезды хакеров и конференции по информационной безопасности, а также методом «снежного кома», когда тех, кто уже принял участие в интервью, просили распространить информацию о проводимом исследовании через своих знакомых. Среди участников 40 % имели опыт незаконного участия в социальной инженерии, остальные 60 % относились к категории «белых хакеров». На основе анализа полученной информации были выделены 12 факторов, влияющих на успех социоинженерной атаки, разделенные на четыре категории:

1) планирование: исследование/разведка, опыт и навыки злоумышленника, а также временные обстоятельства (текущие события, время дня, время года) — контекст атаки [11, 15]. Примером такого контекста может являться пандемия COVID-19 [9–11], активно используемая в качестве предлога для атаки за период 2020–2021;
2) приближение: формирование отношений, сетевая интеграция — изучение социального окружения;

3) побуждение к желаемым действиям — создание активных предлогов: просьба о помощи и поощрение содействия;
4) сокрытие: ситуационная достоверность, непримечательность/обыденность, постановочность (вызов сильных эмоций, срочность, перегрузка информацией), эффективность, приспосабливаемость. Ожидается, что учет в математической модели оценки защищенности пользователя от социоинженерной атаки данных факторов будет способствовать ее уточнению.

Выделенные категории соответствуют четырём этапам модели цикла социоинженерной атаки, предложенной Митником [16].

2.2. Модели цикла социоинженерной атаки

Одной из наиболее известных моделей социальной инженерии является модель атаки Митника [16], основывающаяся на четырёх этапах: исследование, установление контактов, использование контактов и использование полученной информации. При этом если использование полученной информации не ведёт к цели атаки, то предыдущие шаги можно повторить. Авторами [8] данная модель была доработана: добавлены этапы формулирования (определения целей атаки) и подготовки атаки (рис. 1), каждый из представленных этапов, в свою очередь, может содержать подэтапы. Так, например, этап «сбор информации» содержит в себе: определение всех возможных источников, сбор информации из них и оценку полученных сведений. Отметим, что «достижение цели» не рассматривается в качестве отдельного этапа атаки, а лишь является конечной точкой её завершения.

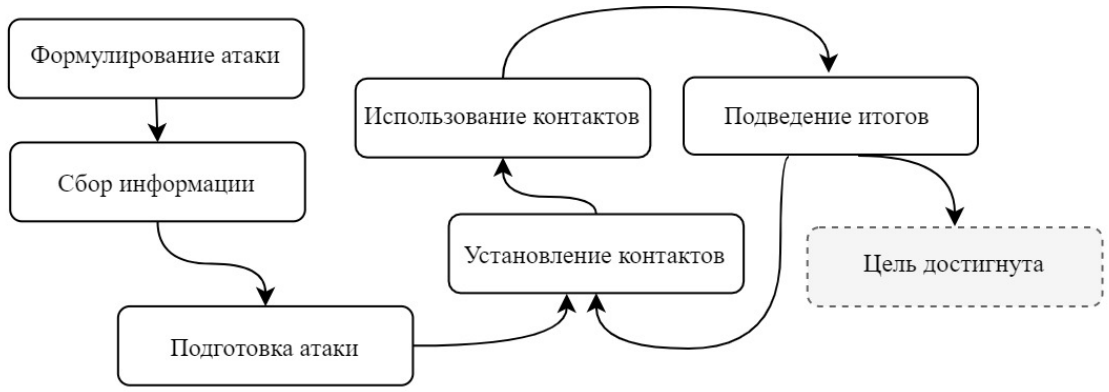

Рис. 1. Модель цикла социоинженерной атаки [8]

Схожий цикл социоинженерной атаки был предложен в [17]. Целью статьи [17] являлся анализ набора реальных сценариев социоинженерных атак, собранных на основе информации, размещаемой в новостях, опубликованной литературе, официальных рекомендациях из отделов безопасности на английском и китайском языках. В результате анализа авторы выделили атрибуты, стратегии и условия, ведущие к успеху социоинженерной атаки. Предлагаемая в [17] основа для анализа социоинженерных атак состоит из следующих этапов: сбор информации, установление контакта, выполнение атакующего воздействия, убеждение в правдивости атакующего воздействия (психологические манипуляции), достижение цели.

2.3. Подходы и решения по анализу защищённости от социоинженерных атак

Описываемые в предыдущем разделе модели могут быть положены в основу автоматизированных инструментов, нацеленных на анализ защищённости пользователей информационных систем от социоинженерных атак.

Пример концепции фреймворка социальной инженерии, основанной на графе атак, а также на моделировании сеансов социальной инженерии и диалогов социальной инженерии предложен в [7]. Авторы предлагают интерпретировать социоинженерную атаку как сеанс, который состоит из нескольких хорошо организованных и тесно связанных между собой диалогов. «Диалог социоинженерной атаки» — это «атомарная атака», которая представляет собой единую связь между злоумышленником и целью. А «сеанс социальной инженерии» — упорядоченная комбинация одного или нескольких диалогов. Для определения сеансов и диалогов используется граф атак, основывающийся на атрибутах.

Исследования [18–20] направлены на анализ атакующих воздействий злоумышленника-социоинженера. В частности, в [19] представлен метод обнаружения атак социальной инженерии, основанный на обработке естественного языка и классификации сообщений при помощи обученных нейронных сетей. В [19] также рассматриваются вопросы создания автоматизированной системы распознавания атак социальной инженерии через чат в корпоративных средах, основывающийся на распознавании личности, распознавании обмана и истории чата. Недостатком данных инструментов является то, что они не учитывают личностные особенности, состояния пользователей, иной влияющий на успех атаки контекст.

2.4. Анализ информации из открытых источников в контексте социоинженерных атак

Одной из часто реализующихся угроз информационной безопасности является самораскрытие информации. Так исследователи [21, 22] описывают «парадокс конфиденциальности», заключающийся в том, что большинство людей, обеспокоенных конфиденциальностью своих личных данных, часто добровольно раскрывают информацию другим. Например, в [21] проводилось исследование сравнивающее самоотчеты пользователей об их реальном поведении и их фактическое поведение в отношении конфиденциальности собственных данных. Для оценки последнего участникам эксперимента предложили выбрать для скачивания одно из мобильных приложений, запрашивающих разный набор разрешений на доступ к данным пользователя. По итогам эксперимента 95 % респондентов установили приложение, запрашивающее разрешения, не связанные с его функциональностью, и только 5 % участников выбрали приложение, которое не запрашивало никаких разрешений. В [22] исследуется парадокс конфиденциальности в контексте социальных сетей (OSN — Online Social Network). Результаты анализа показали, что респонденты считают удобство и функциональность пользования социальными сетями более важными факторами, чем необходимость контролировать параметры конфиденциальности. Оба этих исследования ещё раз подчёркивают актуальность и важность учёта поведения пользователей при мониторинге информационной безопасности. Также существует ряд работ [23–25], направленных на исследование того, что влияет на пользователей при нарушении политики информационной безопасности с психологической точки зрения. В [24] выделяются некоторые черты личности, связанные с безопасностью. В [23] была предложена структура анализа рисков в контексте социоинженерных атак, основанная на профилировании пользо-

вателей. Профилирование пользователей предлагается реализовать путём анализа поведения пользователей сети. Для этого рассматриваются следующие характеристики: частота работы пользователя с email, браузером, загрузками, набор показателей осведомлённости пользователя о различных утечках, набор вероятностей оценки степеней защиты от СИА (phish, waterholing, malware, pop-up) и т. п. В [25] рассматриваются различные атрибуты, которые делятся на такие группы как социально-психологические (черты характера, возраст, пол, образование, знание компьютера, культура), привычки (уровень вовлеченности в социальные сети), социально-эмоциональные (мотивация к использованию социальных сетей, доверие к провайдеру, доверие к членам сети), перцептивные (самоэффективность, воспринимаемый риск, воспринимаемая серьёзность, воспринимаемая вероятность, прошлый опыт, осведомлённость о конфиденциальности, осведомлённость о безопасности). Все данные исследования полезны для построения профиля уязвимостей пользователя, поскольку позволяют учитывать более широкий круг личностных характеристик и выделять те из них, которые наиболее важны с точки зрения информационной безопасности. При этом личностные (в частности, психологические) характеристики зачастую могут быть связаны с online-поведением пользователей в социальных сетях, а именно с характеристиками данных, выкладываемых ими в открытом доступе на своей странице [26, 27]. Разработка системы защиты пользователей организации от социоинженерных атак может задействовать наработки по анализу данных, размещаемых сотрудниками организаций в открытых источниках, в частности, на веб-сайте организации [28], а также инструменты по автоматизированному поиску аккаунтов сотрудников компании в социальных сетях [5]. Такие сведения зачастую изучаются злоумышленником на этапе «сбора информации» и имеют существенное влияние на успех атаки [14]. Кроме того, существует ряд работ по сопоставлению профилей пользователей в нескольких социальных сетях, целью которых является агрегации большего числа сведений, полезных с точки зрения оценки защищенности пользователя от социоинженерной атаки [29–32]. В частности, в [29] предлагается сопоставление аккаунтов в условиях ограниченности исходных данных (используется имя пользователя и список его друзей), в [30, 33] предлагаются алгоритмы сопоставления, базирующиеся на информации, полученной при помощи обработки естественного языка и интеллектуального анализа текста. Также на данном этапе могут быть применены подходы по восстановлению недостающих анкетных данных, например, определение возраста пользователей [34] или подходы по прогнозированию частоты поведения человека [27]. Внедрение данных подходов, методов и алгоритмов в программный комплекс позволит собирать наиболее полную информацию об организации и её сотрудниках, представленных в открытых источниках.

3. МОДЕЛЬ ЦИКЛА СОЦИОИНЖЕНЕРНОЙ АТАКИ

Опишем концептуальную модель цикла социоинженерной атаки в целях последующего использования при разработке программного комплекса для анализа защищенности пользователей информационной системы от социоинженерных атак (рис. 2).

Для последующего моделирования действий злоумышленника этап «формулирование атаки», предлагаемый в [8], предлагается свести к выбору цели атаки злоумышленника (рис. 2). Для этого могут быть введены категории потенциальных объектов атаки, каждый из которых предлагается ассоциировать с сотрудниками, имеющими к ней доступ. Для автоматизации этапа «сбор информации» могут быть использованы работы,

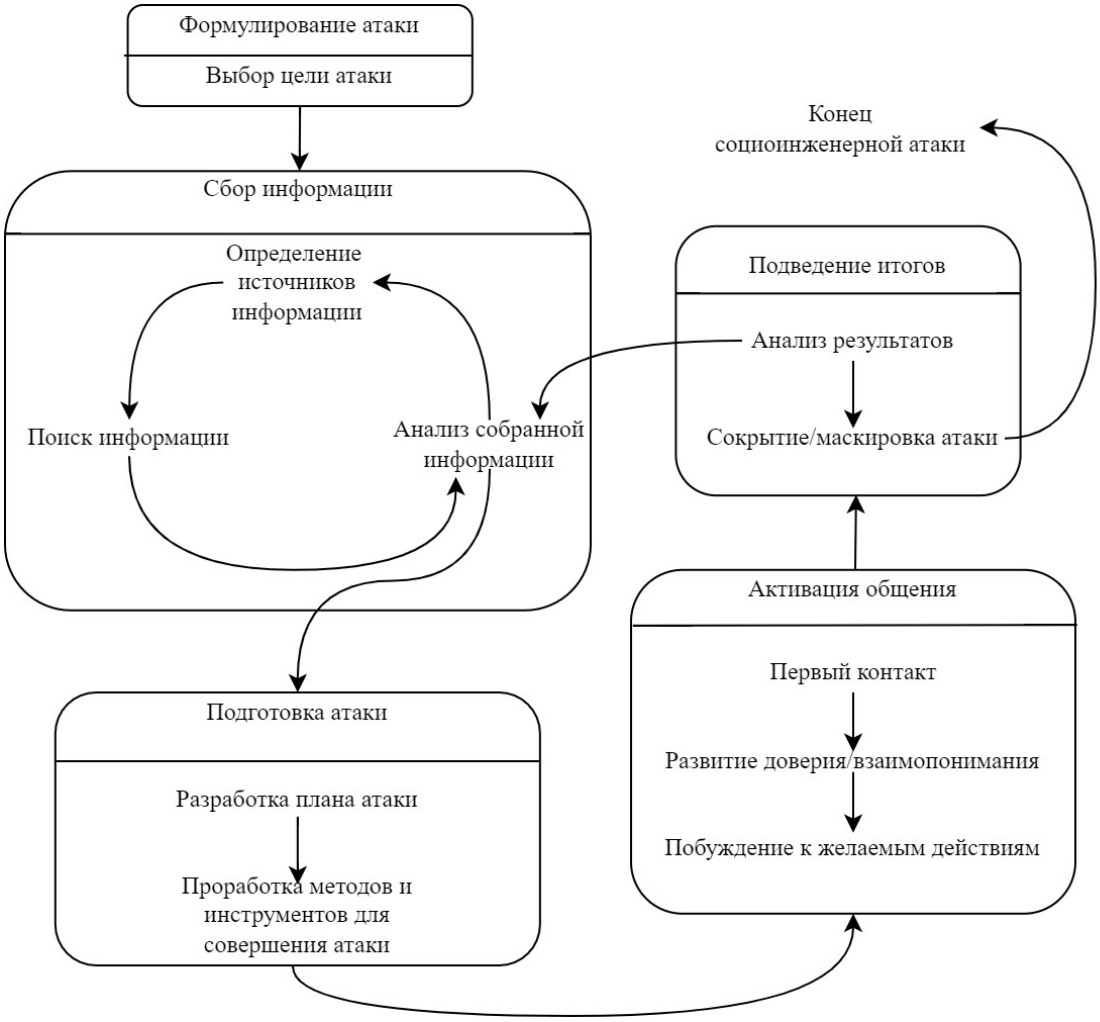

Рис. 2. Предлагаемая модель цикла социоинженерной атаки

описываемые в разделе 2.4. Следующим этапом в модели цикла социоинженерной атаки является «подготовка атаки»: разработка плана атаки и проработка методов и инструментов для совершения атаки. Для проработки мер защиты по данному этапу необходима модель злоумышленника, включающая его компетенции, а также атакующие воздействия, которые им могут быть использованы [5, 15]. Этапы «установление контактов» и «использование контактов» предлагается объединить в «активация общения». Данный этап является одним из ключевых, потому как именно на нём происходит побуждение атакуемого лица к разглашению интересующей критичной информации или действию желаемым образом.

Обобщённая модель функциональности системы с точки зрения конечного пользователя представлена на рисунке 3.

Архитектура программного модуля, соответствующего предложенной модели, представлена на рисунке 4. На ней приведены классы, отвечающие за задание профиля злоумышленника (характеризуется инструментом, который будет использован, и выбранной для атаки целью — категория объекта), набор существующих инструментов для атаки, связанный с набором механизмов воздействия, которым, в свою очередь, сопоставле-

Рис. 3. Диаграмма использования

ны уязвимости, на которые они могут оказать влияние. Также представлен класс, характеризующий пользователя со списком доступных ему категорий объектов. При запуске программы пользователю будет предложено внести необходимые данные, выбрать цель атаки злоумышленника и инструмент и запустить анализ организации. При этом функция анализа реализует поиск пользователей, имеющих доступ к выбранной цели атаки, а также с наибольшей выраженностью тех уязвимостей, которые могут быть активированы выбранным инструментом для атаки, в качестве выходных данных будет выдан упорядоченный набор пользователей, наиболее уязвимых при заданной атаке.

4. ЗАКЛЮЧЕНИЕ

Таким образом, в работе был представлен обзор существующих исследований в контексте социоинженерных атак, размещённых в базе Web of Science за последние 3 года. Для обзора были отобраны исследования, посвящённые анализу защищённости пользователей от социоинженерных атак. Были выделены как общие концепции моделирования социоинженерных атак, так и частные реализации, в том числе связанные с учётом психологических особенностей при анализе подверженности социоинженерным атакам и информацией, выкладываемой в социальных сетях. Результатом работы является построение на основе сделанного обзора концептуальной модели цикла социоинженерной атаки, а также предложение архитектуры прототипа программного комплекса, преимуществом которого является учёт профиля злоумышленника и набора существующих инструментов для атаки. Практическая значимость заключается в создании основы для разработки программного решения для моделирования социоинженерной атаки и последующего выявления наиболее уязвимых сотрудников организации к социоинженерным атакам, учитывающего сведения о потенциальном объекте атаки. В качестве дальнейшего развития исследований предполагается проработка связи текущей архитектуры прототипа программного комплекса с инструментами сбора информации о сотрудниках организации из открытых источников.

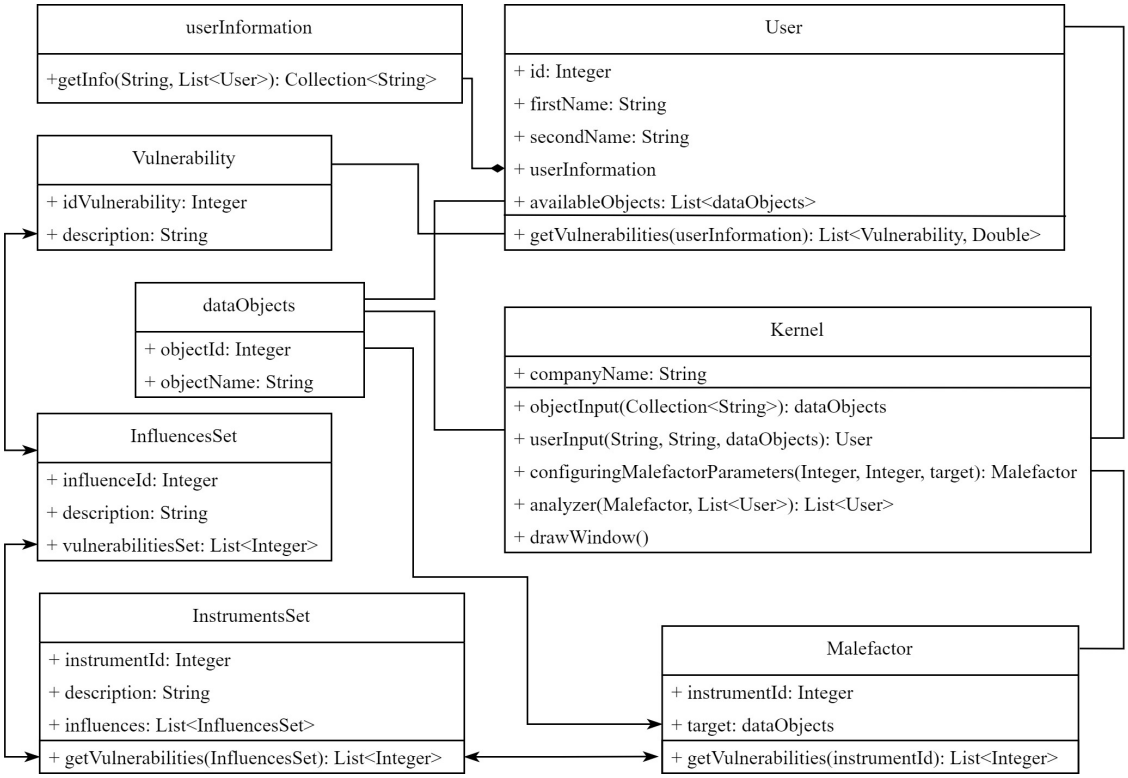

Рис. 4. Архитектура прототипа программного комплекса

Список литературы

1. Federal Bureau of Investigation “IC3 Logs 6 Million Complaints. Record Increase in Reporting Brings IC3 to New Milestone”. [Электронный ресурс] URL: https://www.fbi.gov/news/stories/ic3-logs-6-million-complaints-051721 (дата доступа: 23.09.2021).
2. *Snyman D., Kruger H. A.* External contextual factors in information security behaviour. 2020. P. 185–194. doi: 10.5220/0009142201850194
3. *Wang Z., Sun L., Zhu H.* Defining social engineering in cybersecurity // IEEE Access. Vol. 8. P. 85094–85115. doi: 10.1109/ACCESS.2020.2992807
4. *Salahdine F., Kaabouch N.* Social engineering attacks: A survey // Future Internet. 2019. Vol. 11, № 4. P. 89. doi: 10.3390/fi11040089
5. *Абрамов М. В., Тулупьева Т. В., Тулупьев А. Л.* Социоинженерные атаки: социальные сети и оценки защищенности пользователей. СПб.: ГУАП, 2018. 266 с.
6. Weekly Threat Report 30th July 2021 [Электронный ресурс] URL: https://www.ncsc.gov.uk/report/weekly-threat-report-30th-july-2021 (дата доступа: 23.09.2021).
7. *Zheng K., Wu T., Wang X., Wu B., Wu C.* A session and dialogue-based social engineering framework // IEEE Access. 2019. Vol. 7. P. 67781–67794. doi: 10.1109/ACCESS.2019.2919150
8. *Mouton F., Leenen L., Venter H.S.* Social engineering attack examples, templates and scenarios // Computers & Security. 2016. Vol. 59. P. 186–209. doi: 10.1016/j.cose.2016.03.004
9. *Hijji M., Alam G.* A Multivocal Literature Review on Growing Social Engineering Based Cyber-Attacks/Threats During the COVID-19 Pandemic: Challenges and Prospective Solutions // IEEE Access. 2021. Vol. 9. P. 7152–7169. doi: 10.1109/ACCESS.2020.3048839
10. *Gryszczynska A.* The impact of the COVID-19 pandemic on cybercrime //Bulletin of the Polish Academy of Sciences. Technical Sciences. 2021. Vol. 69, № 4. P. e137933. doi: 10.24425/bpasts.2021.137933
11. *Naidoo R.* A multi-level influence model of COVID-19 themed cybercrime // European Journal of Information Systems. 2020. Vol. 29, № 3. P. 306–321. doi: 10.1080/0960085X.2020.1771222

12. *Wang, Z., Zhu, H., Liu, P., & Sun, L.* Social Engineering in Cybersecurity: A Domain Ontology and Knowledge Graph // CYBERSECURITY. 2021. Vol. 4, № 31. doi: 10.1186/s42400-021-00094-6
13. Bullee J. W., Junger M. How effective are social engineering interventions? A meta-analysis // Information & Computer Security. 2020. Vol. 28, № 5. P. 801–830. doi: 10.1108/ICS-07-2019-0078
14. *Steinmetz K. F., Pimentel A., Goe W. R.* Performing social engineering: A qualitative study of information security deceptions // Computers in Human Behavior. 2021. Vol. 124. P. 106930. doi: 10.1016/j.chb.2021.106930
15. *Wang Z., Zhu H., Sun L.* Social Engineering in Cybersecurity: Effect Mechanisms, Human Vulnerabilities and Attack Methods // IEEE Access. 2021. Vol. 9. P. 11895–11910. doi: 10.1109/ACCESS.2021.3051633
16. *Mitnick K. D., Simon W. L.* The art of deception: Controlling the human element of security. John Wiley & Sons, 2003. 351 p.
17. *Yasin A., Fatima R., Liu L., Wang J., Ali R., Wei Z.* Understanding and deciphering of social engineering attack scenarios // Security and Privacy. 2021. Vol. 4, № 4. P. e161. doi: 10.1002/spy2.161
18. *Aldawood H., Skinner G.* An academic review of current industrial and commercial cyber security social engineering solutions // Proceedings of the 3rd International Conference on Cryptography, Security and Privacy. 2019. P. 110–115. doi: 10.1145/3309074.3309083
19. *Lansley M., Mouton F., Kapetanakis S., Polatidis N.* SEADer plus plus: social engineering attack detection in online environments using machine learning // Journal of Information and Telecommunication. 2020. Vol. 4, № 3. P. 346–362. doi: 10.1080/24751839.2020.1747001
20. *Tsinganos N., Sakellariou G., Fouliras P., Mavridis I.* Towards an automated recognition system for chat-based social engineering attacks in enterprise environments // Proceedings of the 13th International Conference on Availability, Reliability and Security. 2018. P. 1–10. doi: 10.1145/3230833.3233277
21. *Barth S., de Jong M.D., Junger M., Hartel P.H., Roppelt J.C.* Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources // Telematics and informatics. 2019. Vol. 41. P. 55–69. doi: 10.1016/j.tele.2019.03.003
22. *Kuzmanovic M., Savic G.* Avoiding the Privacy Paradox Using Preference-Based Segmentation: A Conjoint Analysis Approach // Electronics. 2020. Vol. 9, № 9. P. 1382. doi: 10.3390/electronics9091382
23. *Ye Z., Guo Y., Ju A., Wei F., Zhang R., Ma J.* A Risk Analysis Framework for Social Engineering Attack Based on User Profiling // Journal of Organizational and End User Computing (JOEUC). 2020. Vol. 32, № 3. P. 37–49. doi: 10.4018/JOEUC.2020070104
24. *Moustafa A. A., Bello A., Maurushat A.* The role of user behaviour in improving cyber security management. Frontiers in Psychology. V. 12. 561011. doi: 10.3389/fpsyg.2021.561011
25. *Albladi S. M., Weir G. R. S.* User characteristics that influence judgment of social engineering attacks in social networks // Human-centric Computing and Information Sciences. 2018. Vol. 8, № 1. P. 1–24. doi: 10.1186/s13673-018-0128-7
26. *Edwards M., Larson R., Green B., Rashid A., Baron A.* Panning for gold: Automatically analysing online social engineering attack surfaces. Computers & Security. Vol. 69. P. 18–34. doi: 10.1016/j.cose.2016.12.013
27. *Toropova A., Tulupyeva T.* Comparison of Behavior Rate Models Based on Bayesian Belief Network // International Scientific and Practical Conference in Control Engineering and Decision Making. Springer, Cham, 2020. P. 510–521. doi: 10.1007/978-3-030-65283-8_42
28. *Wang J., Wang X., Zhang H., Fang B., Yang Y., Liu J.* Information Classification and Extraction on Official Web Pages of Organizations // CMC-COMPUTERS MATERIALS & CONTINUA. 2020. Vol. 64, № 3. P. 2057–2073. doi: 10.32604/cmc.2020.011158
29. *Nurgaliev I., Qu Q., Bamakan S. M. H., Muzammal M.* Matching user identities across social networks with limited profile data // Frontiers of Computer Science. 2020. Vol. 14, № 6. P. 1–14. doi: 10.1007/s11704-019-8235-9
30. *Srivastava D. K., Roychoudhury B.* Words are important: A textual content based identity resolution scheme across multiple online social networks // Knowledge-Based Systems. 2020. Vol. 195. P. 105624. doi: 10.1016/j.knosys.2020.105624
31. *Wang L., Hu K., Zhang Y., Cao S.* Factor Graph Model Based User Profile Matching Across Social Networks // IEEE Access. 2019. Vol. 7. P. 152429–152442. doi: 10.1109/ACCESS.2019.2948073

32. *Li Y., Zhang Z., Peng Y., Yin H., Xu Q.* Matching user accounts based on user generated content across social networks // Future Generation Computer Systems. 2018. Vol. 83. P. 104–115. doi: 10.1016/j.future.2018.01.041
33. *Oliseenko V. D., Tulupyeva T. V.* Neural network approach in the task of multi-label classification of user posts in online social networks // 2021 XXIV International Conference on Soft Computing and Measurements (SCM). IEEE, 2021. P. 46–48. doi: 10.1109/SCM52931.2021.9507148
34. *Oliseenko V., Korepanova A.* How old users are? Community analysis // CEUR Workshop Proceedings. RWTH Aahen University, 2020. Vol. 2782. P. 246–251.

Поступила в редакцию 20.08.2021, окончательный вариант — 23.09.2021.

Хлобыстова Анастасия Олеговна, младший научный сотрудник, Санкт-Петербургский Федеральный исследовательский центр Российской академии наук (СПб ФИЦ РАН), 14 линия, 39, 199178, Санкт-Петербург, Россия, ✉ aok@dscs.pro

Computer tools in education, 2021
№ 3: 17–28
http://cte.eltech.ru
doi:10.32603/2071-2340-2021-3-17-28

Conceptual Model of the Social Engineering Attack Cycle: Modern Approaches and Software Prototype Architecture

Khlobystova A. O.[1], PhD, Associate Professor, ✉ aok@dscs.pro

[1]St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS), 14-th Linia, VI, № 39, St. Petersburg, 199178, Russia, https://dscs.pro/

Abstract

Social engineering attacks are one of the key problems of our time. Every year, their number and efficiency continue to grow. This paper provides an overview of existing studies devoted to the problem of protecting users from social engineering attacks. On the basis of the review, a conceptual model of the social engineering attack cycle and the architecture of a prototype software are proposed, the advantage of which over existing analogues is the account of the malefactor's profile and a set of existing attack tools. The practical significance lies in creating a basis for developing a software solution for simulating the social engineering attacks and subsequent identification the most vulnerable employees of an organization to social engineering attacks, taking into account information about a potential target of an attack.

Keywords: *social engineering attacks, social engineering attack cycle model, user vulnerability profile, malefactor profile.*

Citation: A. O. Khlobystova, "Conceptual Model of the Social Engineering Attack Cycle: Modern Approaches and Software Prototype Architecture," *Computer tools in education*, no. 3, pp. 17–28, 2021 (in Russian); doi: 10.32603/2071-2340-2021-3-17-28

Acknowledgements: *The research was carried out in the framework of the project on state assignment SPC RAS №0073-2019-0003; with the financial support of the RFBR №20-07-00839.*

References

1. Federal Bureau of Investigation "IC3 Logs 6 Million Complaints. Record Increase in Reporting Brings IC3 to New Milestone," in *fbi.gov*, [News], 14 May 2021. [Online]. Available: https://www.fbi.gov/news/stories/ic3-logs-6-million-complaints-051721
2. D. Snyman and H. Kruger, "External Contextual Factors in Information Security Behaviour," in *Proc. of the 6th Int. Conf. on Information Systems Security and Privacy — ICISSP, Valletta, Malta, 2020*, 2020, pp. 185–194; doi: 10.5220/0009142201850194
3. Z. Wang, L. Sun, and H. Zhu, "Defining social engineering in cybersecurity," *IEEE Access*, vol. 8, pp. 85094–85115, 2002; doi: 10.1109/ACCESS.2020.2992807
4. F. Salahdine, N. Kaabouch, "Social engineering attacks: A survey," *Future Internet*, vol. 11, no. 4, pp. 89, 2019; doi: 10.3390/fi11040089
5. M. V. Abramov, T. V. Tulupyeva, A. L. Tulupyev, *Sotsioinzhenernye ataki: sotsial'nye seti i otsenki zashchishchennosti pol'zovatelei* [Social engineering attacks: social networks and user security assessments], St. Petersburg: GUAP, 2018 (in Russian).
6. The National Cyber Security Centre, "Weekly Threat Report 30th July 2021," in *ncsc.gov.uk*, [Report], 30 Jul. 2021. [Online]. Available:https://www.ncsc.gov.uk/report/weekly-threat-report-30th-july-2021
7. K. Zheng, T. Wu, X. Wang, B. Wu, and C. Wu, "A Session and Dialogue-Based Social Engineering Framework," *IEEE Access*, vol. 7, pp. 67781–67794, 2019; doi: 10.1109/ACCESS.2019.2919150
8. F. Mouton, L. Leenen, and H. S. Venter, "Social engineering attack examples, templates and scenarios," *Computers & Security*, vol. 59, pp. 186–209, 2016; doi: 10.1016/j.cose.2016.03.004
9. M. Hijji and G. Alam, "A Multivocal Literature Review on Growing Social Engineering Based Cyber-Attacks/Threats During the COVID-19 Pandemic: Challenges and Prospective Solutions," *IEEE Access*, vol. 9, pp. 7152–7169, 2021; doi: 10.1109/ACCESS.2020.3048839
10. A. Gryszczynska, "The impact of the COVID-19 pandemic on cybercrime" *Bulletin of the Polish Academy of Sciences. Technical Sciences*, vol. 69, no. 4, p. e137933, 2021; doi: 10.24425/bpasts.2021.137933
11. R. Naidoo, "A multi-level influence model of COVID-19 themed cybercrime," *European Journal of Information Systems*, vol. 29, no. 3, pp. 306–321, 2020; doi: 10.1080/0960085X.2020.1771222
12. Z. Wang, H. Zhu, P. Liu, and L. Sun, "Social engineering in cybersecurity: a domain ontology and knowledge graph application examples," *Cybersecurity*, vol. 4, no. 1, 2021; doi: 10.1186/s42400-021-00094-6
13. J.-W. Bullee and M. Junger, "How effective are social engineering interventions? A meta-analysis," *Information & Computer Security*, vol. 28, no. 5, pp. 801–830, 2020; doi: 10.1108/ICS-07-2019-0078
14. K. F. Steinmetz, A. Pimentel, and W. R. Goe, "Performing social engineering: A qualitative study of information security deceptions," *Computers in Human Behavior*, vol. 124, p. 106930, 2021; doi: 10.1016/j.chb.2021.106930
15. Z. Wang, H. Zhu, and L. Sun, "Social Engineering in Cybersecurity: Effect Mechanisms, Human Vulnerabilities and Attack Methods," *IEEE Access*, vol. 9, pp. 11895–11910, 2021; doi: 10.1109/ACCESS.2021.3051633
16. K. D. Mitnick and W. L. Simon, *The art of deception: Controlling the human element of security*, Indianapolis, IN, USA: John Wiley & Sons, 2003.
17. A. Yasin, R. Fatima, L. Liu, J. Wang, R. Ali, and Z. Wei, "Understanding and deciphering of social engineering attack scenarios," *Security and Privacy*, vol. 4, no. 4, pp. e161, 2021; doi: 10.1002/spy2.161
18. H. Aldawood and G. Skinner, "An academic review of current industrial and commercial cyber security social engineering solutions," in *Proc. of the 3rd International Conference on Cryptography, Security and Privacy — ICCSP'19*, 2019. pp. 110–115; doi: 10.1145/3309074.3309083
19. M. Lansley, F. Mouton, S. Kapetanakis, and N. Polatidis, "SEADer++: social engineering attack detection in online environments using machine learning," *Journal of Information and Telecommunication*, vol. 4, no. 3, pp. 346–362, 2020; doi: 10.1080/24751839.2020.1747001
20. N. Tsinganos, G. Sakellariou, P. Fouliras, and I. Mavridis, "Towards an Automated Recognition System for Chat-based Social Engineering Attacks in Enterprise Environments," in *Proc. of the 13th International Conference on Availability, Reliability and Security, Aug. 2018*, 2018, pp. 1–10; doi: 10.1145/3230833.3233277
21. S. Barth, M. D. T. de Jong, M. Junger, P. H. Hartel, and J. C. Roppelt, "Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources," *Telematics and Informatics*, vol. 41, pp. 55–69, 2019; doi: 10.1016/j.tele.2019.03.003
22. S. Barth, M. D. T. de Jong, M. Junger, P. H. Hartel, and J. C. Roppelt, "Putting the privacy paradox to the test: Onli-

ne privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources," *Telematics and Informatics*, vol. 41, pp. 55–69, 2019; doi: 10.3390/electronics9091382
23. Z. Ye, Y. Guo, A. Ju, F. Wei, R. Zhang, and J. Ma, "A Risk Analysis Framework for Social Engineering Attack Based on User Profiling," *Journal of Organizational and End User Computing*, vol. 32, no. 3, pp. 37–49, 2020; doi: 10.4018/JOEUC.2020070104
24. A. A. Moustafa, A. Bello, and A. Maurushat, "The Role of User Behaviour in Improving Cyber Security Management," *Frontiers in Psychology*, vol. 12, article 561011, 2021; doi: 10.3389/fpsyg.2021.561011
25. S. M. Albladi and G. R. S. Weir, "User characteristics that influence judgment of social engineering attacks in social networks," *Human-centric Computing and Information Sciences*, vol. 8, no. 1, pp. 1–24, 2018; doi: 10.1186/s13673-018-0128-7
26. M. Edwards, R. Larson, B. Green, A. Rashid, and A. Baron, "Panning for gold: Automatically analysing online social engineering attack surfaces," *Computers & Security*, vol. 69, pp. 18–34, 2017; doi: 10.1016/j.cose.2016.12.013
27. A. Toropova and T. Tulupyeva, "Comparison of Behavior Rate Models Based on Bayesian Belief Network," in *Recent Research in Control Engineering and Decision Making. ICIT 2020. Studies in Systems, Decision and Control*, vol. 337, pp. 510–521, 2020; doi: 10.1007/978-3-030-65283-8_42
28. J. Wang, X. Wang, H. Zhang, B. Fang, Y. Yang, and J. Liu, "Information Classification and Extraction on Official Web Pages of Organizations," *Computers, Materials & Continua*, vol. 64, no. 3, pp. 2057–2073, 2020; doi: 10.32604/cmc.2020.011158
29. I. Nurgaliev, Q. Qu, S. M. H. Bamakan, and M. Muzammal, "Matching user identities across social networks with limited profile data," *Frontiers of Computer Science*, vol. 14, no. 6, pp. 1–14, 2020; doi: 10.1007/s11704-019-8235-9
30. D. K. Srivastava and B. Roychoudhury, "Words are important: A textual content based identity resolution scheme across multiple online social networks," *Knowledge-Based Systems*, vol. 195, p. 105624, 2020; doi: 10.1016/j.knosys.2020.105624
31. L. Wang, K. Hu, Y. Zhang, and S. Cao, "Factor Graph Model Based User Profile Matching Across Social Networks," *IEEE Access*, vol. 7, pp. 152429–152442, 2019; doi: 10.1109/ACCESS.2019.2948073
32. Y. Li, Z. Zhang, Y. Peng, H. Yin, and Q. Xu, "Matching user accounts based on user generated content across social networks," *Future Generation Computer Systems*, vol. 83, pp. 104–115, 2018; doi: 10.1016/j.future.2018.01.041
33. V. D. Oliseenko and T. V. Tulupyeva, "Neural Network Approach in the Task of Multi-label Classification of User Posts in Online Social Networks," in *Proc. of XXIV Int. Conf. on Soft Computing and Measurements (SCM), May 2021*, 2021, pp. 46–48; doi: 10.1109/SCM52931.2021.9507148
34. V. Oliseenko and A. Korepanova, "How old users are? Community analysis," in *CEUR Workshop Proc. RWTH Aahen University*, vol. 2782, 2020, pp. 246–251.

Received 20-08-2021, the final version — 23-09-2021.

20.08.2021 23.09.2021

Khlobystova Anastasiia Olegovna, St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS),14-th Linia, VI, № 39, St. Petersburg, 199178, Russia, https://dscs.pro/, ✉ **aok@dscs.pro**