Адаптация модели многоходовых социоинженерных атак с учётом информационного влияния

А. О. Хлобыстова
Санкт-Петербургский Федеральный исследовательский центр Российской академии наук (СПб ФИЦ РАН)
aok@dscs.pro

М. В. Абрамов
Санкт-Петербургский Федеральный исследовательский центр Российской академии наук (СПб ФИЦ РАН)
mva@dscs.pro

***Аннотация*. Рост уровня и числа социоинженерных атак требует разработки действенных мер по их предотвращению. Одной из таких мер является анализ социального графа сотрудников организации, направленный на выявление наиболее уязвимых с точки зрения информационной безопасности пользователей и/или цепочек пользователей, чтобы впоследствии предпринять меры по повышению уровня защищенности. Целью настоящей работы является адаптация имеющихся математических моделей оценки вероятности успеха распространения многоходовых социоинженерных атак, позволяющая учитывать силу информационного влияния, то есть воздействия на поведение пользователей информационной системы его окружением.1Предлагаемый подход основывается на модели расчёта влияния агента и модели многоходовой социоинженерной атаки. Настоящее исследование может быть использовано при анализе социального графа сотрудников организации и опосредовано даёт возможность принимать таргетированные меры по повышению уровня защищённости организации от социоинженерных атак.**

Ключевые слова: социоинженерные атаки; социальный граф, интенсивность взаимодействия пользователей, модель информационного влияния

I. Введение

Социальная инженерия уже долгое время остаётся одним из наиболее эффективных методов, используемых при атаках с целью нарушения политик информационной безопасности организаций. Данный тип кибератаки обычно трудно распознать как отдельно взятому пользователю, на которого совершается атака, так и целому отделу сотрудников службы информационной безопасности организации, поскольку цифровые технологии играют роль вспомогательных инструментов, а сами атаки базируются на особенностях психологии людей, учесть которые достаточно сложно.

Прошедший 2020 год предоставил массу новых предлогов и сценариев для осуществления социоинженерных атак [1], [2], [3] – самоизоляция, дистанционная работа, ограничения личных встреч привели к ещё большей зависимости от технологий виртуального взаимодействия [4]. Так по данным группы аналитики угроз Microsoft уже через неделю после заявления ВОЗ о чрезвычайной ситуации число социоинженерных атак, связанных с темой COVID, увеличилось в 11 раз [5]. При этом пандемия является всего лишь одним из предлогов, который используют злоумышленники. Эксперты отмечают, что социоинженерные атаки с каждым годом становятся все более распространенными и изощренными [6], [7].

Нередким явлением при совершении социоинженерных атак является сбор информации об атакуемой компании из открытых источников, включая поиск аккаунтов её сотрудников в социальных сетях [8]. При этом злоумышленники стремятся выявить наиболее уязвимого к атаке пользователя [9], после чего уже через него осуществлять дальнейшие атакующие воздействия, например, узнав больше сведений об организационной структуре компании или при помощи манипулятивных тактик убедив пользователя выполнить действия, ведущие к нарушению конфиденциальности организации. Вид атак, совершаемый через цепочку пользователей, называется многоходовыми социоинженерными атаками [10]. Одним из способов повышения уровня защищённости организаций к многоходовым социоинженерным атакам является построение социального графа сотрудников организации, узлы которого ассоциированы с пользователями информационной системы, а дуги – связи между ними [10]. Анализ социального графа позволяет выявлять наиболее уязвимые места с точки зрения социоинженерных атак, после чего таргетировованно принимать меры по снижению степени выраженности уязвимостей у пользователей. В свою очередь при анализе социального графа важную роль играет моделирование распространения социоинженерной атаки, которое включает в себя оценки интенсивности связей между пользователями. Одним из способов получения оценки интенсивности межпользовательского общения является модель расчёта влияния. Целью настоящей работы является адаптация имеющихся математических моделей распространения многоходовых социоинженерных атак, позволяющая учитывать силу информационного влияния. Новизна исследования заключается в том, что математическая модель распространения многоходовых социоинженерных атак впервые рассматривается в

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

совокупности с моделью расчёта влияния агентов. Научная значимость работы заключается в развитии математического аппарата для моделирования действий злоумышленника-социоинженера и создании фундамента для последующего анализа социального графа сотрудников организации. Практическая значимость состоит в формировании возможностей лицам, принимающим решения, осуществлять более точные меры по повышению уровня защищённости как отдельных сотрудников, так и организации в целом.

II. Релевантные работы

Заделом для данного исследования послужили работы коллектива авторов Чхартишвили, Губанов [11]–[13]. В данных статьях авторы предлагают модель расчёта влияния агентов (пользователей/сотрудников организации) на основе действий, совершаемых ими в социальной сети ВКонтакте. Описанные модели применялись в контексте выявления каналов распространения информации в социальной сети [12], а также для расчёта уровней влияния участников политического форума социальной сети reddit.com [13]. В настоящем исследовании предлагается применить модель расчёта влияния агентов в контексте социоинженерных атак.

Также заделом для данного исследования послужили работы [10], [14], [15]. В [10] было введено понятие многоходовых социоинженерных атак, реализуемых через цепочку пользователей, предложена модель оценки интенсивности взаимодействия между пользователями, о которых речь пойдёт в III разделе. В [14] был предложен подход к выявлению наиболее критичной траектории распространения социоинженерной атаки. В [15] в качестве оценки интенсивности взаимодействия между пользователями было предложено использовать сведения из профиля пользователя: информацию о родителях, детях, братьях/сестрах, семейное положение и публичные списки друзей; для применения такой информации при анализе социального графа сотрудников организации был применён подход, предложенный Н.В. Хованов.

III. Теоретическая часть

A. Модель информационного влияния

Согласно [11] введём систему обозначений. Под множеством агентов N будем понимать множество пользователей информационной сети $U=\{U_1,\ldots,U_n\}$; K – множество допустимых типов действий; T – дискретное множество, соответствующее рассматриваемому интервалу времени; Δ – множество действий, любое действие $a\in\Delta$ может быть охарактеризовано тройкой вида $a=(U_i,K_i,T_i)$, где U_i – пользователь (агент), который его совершил $(U_i\in U)$, K_i – тип этого действия $(K_i\in K)$, T_i – момент времени, в который данное действие было совершено $(T_i\in T)$; также введём бинарное отношение частичного порядка – отношение причины $a\to b$. Например, действие a – публикация поста в социальной сети пользователем U_i в момент времени T_i, действие b – добавление комментария к этому посту пользователем U_j в момент времени T_j $(T_i<T_j)$, тогда для них можно задать отношение причины $a\to b$.

Для $A\subseteq\Delta$ можно определить множество всех его последствий $\pi(A)=\{b\in\Delta\mid \exists a\in A: a\to b\}$, также среди множества всех действий Δ можно выделить множество $\Delta^0=\{b\in\Delta\mid \exists\, a\in A: a\to b\Rightarrow a=b\}$ – множество первоначальных действий, которые не являются последствием каких-либо других действий.

Кроме того, введём функцию значимости $\Phi: 2^{\Delta}\to[0;+\infty)$ такую, что $\Phi(\Delta)>0$, Φ – монотонная, если $A,B\subseteq\Delta, A\subset B$, то $\Phi(A)\le\Phi(B)$, Φ – аддитивная, $\Phi(A\cup B)=\Phi(A)+\Phi(B)$, $A,B,A\cup B\subseteq\Delta$.

Функция $\alpha:\Delta\to U$ – сопоставляет действию агента, который его совершил.

Функция влияния пользователя U_i на пользователя U_j может быть задана следующим образом:

$$\chi(U_i,U_j)=\begin{cases}\dfrac{\Phi(\pi(\delta^0_{U_i})\cap\delta_{U_j})}{\Phi(\delta_{U_j})}, & \Phi(\delta_{U_j})>0\\ 0, & \Phi(\delta_{U_j})=0\end{cases}, \qquad (1)$$

где $\delta_{U_j}=\{a\in\Delta\mid\exists\,\alpha(a)\in U_j\}$ – множество действий агента $U_j\in U$, $\pi(\delta^0_{U_i})=\{b\in\Delta^0\mid\exists\, a\in\delta_{U_i}: a\to b\}$ – множество действий, которые являются последствиями начальных действия агента $U_i\in U$.

B. Модель распространения многоходовой атаки

Согласно [10] оценка вероятности того, что социоинженерная атака распространится между пользователями рассчитывается по формуле $P=1-Q$, где Q – оценка вероятности того, что социоинженерная атака не распространится между пользователями, учитывающая интенсивности различных видов связи. $Q=\prod_i(1-q_i)^{n_t}$, где q_i – оценка вероятности успеха социоинженерной атаки при одном эпизоде взаимодействия, n_t – число эпизодов.

Q предлагалось рассчитывать следующим образом:

$$Q=(1-p_{\text{rel}})(1-p_{\text{likes}})^{\text{count\_likes}}(1-p_{\text{reposts}})^{\text{count\_reposts}}$$

$$(1-p_{\text{com\_photos}})^{\text{count\_photos}}(1-p_{\text{com\_groups}})^{\text{count\_groups}},$$

где p_{rel} – вероятность успеха распространения атаки от сотрудника к сотруднику, основанная на типе декларируемой в социальной сети связи. В качестве p_{rel} могут быть использованы оценки, полученные в [15].

IV. Применение в контексте социоинженерных атак

На примере социальной сети ВКонтакте рассмотрим объединение описанных выше подходов с целью разработки новой математической модели, позволяющей строить оценки вероятностей распространения социоинженерной атаки между пользователями.

Эпизоды взаимодействия пользователей будем рассматривать как допустимые действия, которые пользователи могут совершить, публично взаимодействуя друг с другом, в социальной сети ВКонтакте. Допустимые действия представлены в таблице.

ТАБЛИЦА I Допустимые действия

Обозначение	Описание
K_1	Публикция поста
K_2	Комментирование поста
K_3	Репост поста
K_4	Лайк поста
K_5	Ответ на комментарий
K_6	Лайк комментария
K_7	Упоминание профиля пользователя в посте
K_8	Отметка на фотографии
K_9	Подарок

Зададим функцию значимости Ф как мощность множества, то есть $A \subseteq \Delta, \Phi(A) = |A|$.

Вероятность успеха социоинженерной атаки при одном эпизоде взаимодействия q_i будем рассчитывать аналогично функции влияния пользователя U_i на пользователя U_j:

$$q_i(U_j) = \chi(U_i, U_j) = \begin{cases} \dfrac{\left|\pi(\delta^0_{U_i}) \cap \delta_{U_j}\right|}{\left|\delta_{U_j}\right|}, & \delta_{U_j} \neq \varnothing \\ 0, & \delta_{U_j} = \varnothing \end{cases}. \qquad (2)$$

При таком задании $\forall U_i, U_j \ \ 0 \le \chi(U_i, U_j) \le 1$. А вероятность того, что социоинженерная атака распространится от пользователя U_i к пользователю U_j будет рассчитываться по формуле $P_{ij} = 1 - (1 - p^{rel}_{ij}) q_i(U_j)$. Отметим, что при таком подходе нет необходимости включать в формулу параметр n_t (число эпизодов), так как все ответные действия пользователя будут учтены в функции влияния.

V. Пример расчёта

U', U'' – пользователи $(U', U'' \in U)$, T', T'' – некоторые моменты времени $(T', T'' \in T)$ такие, что $T' < T''$. Для упрощения записи под $K' \downarrow K''$ будем понимать $(U', K', T') \to (U'', K'', T'')$. С использованием Таблица I зададим пары действий, удовлетворяющие отношению причины $a \to b$: $K_1 \downarrow K_2$, $K_1 \downarrow K_3$, $K_1 \downarrow K_4$, $K_1 \downarrow K_7$, $K_2 \downarrow K_5$, $K_1 \downarrow K_5$, $K_2 \downarrow K_6$, $K_1 \downarrow K_6$, $K_5 \downarrow K_6$.

Рассмотрим взаимодействие на примере 3-х пользователей. Пусть из социальной сети ВКонтакте можно узнать, что у пользователя U_1 пользователь U_2 указан как «лучший друг». Согласно [15] такой вид связи оценивается в $p^{rel}_{12} = 0,7838$. Пусть у U_1 пользователь U_2 есть в списке друзей, тогда по [15] $p^{rel}_{13} = 0,2938$. Пусть также известно, что были совершены следующие действия $\Delta = \{(U_1, K_1, T_1), (U_1, K_7, T_2), (U_2, K_4, T_3), (U_2, K_2, T_4), (U_3, K_2, T_5)\}, T_1 \le T_2 \le T_3 \le T_4 \le T_5$.

Известно множество начальных действий U_1 $\delta^0_{U_1} = \{(U_1, K_1, T_1)\}$, и множество последствий: $\pi(\delta^0_{U_1}) = \{(U_1, K_1, T_1), (U_1, K_7, T_2), (U_2, K_4, T_3), (U_2, K_2, T_4), (U_3, K_2, T_5)\}$, действия U_2: $\delta_{U_2} = \{(U_2, K_4, T_3), (U_2, K_2, T_4)\}$, действия U_3: $\delta_{U_3} = \{(U_3, K_2, T_5), (U_3, K_1, T_6)\}$.

Тогда вероятность того, что социоинженерная атака распространится от пользователя U_1 к пользователю U_2 будет рассчитываться следующим образом:

$$P_{12} = 1 - (1 - 0,7838) \cdot \frac{\left|\pi(\delta^0_{U_1}) \cap \delta_{U_2}\right|}{\left|\delta_{U_2}\right|} =$$

$$= 1 - (1 - 0,7838) \cdot 1 = 0,7838.$$

$$P_{13} = 1 - (1 - 0,2938) \cdot 0,5 = 0,6469.$$

Таким образом, согласно полученной модели, вероятность распространения социоинженерной атаки от пользователя U_1 к пользователю U_2 выше, чем от U_1 к U_3.

VI. Заключение

Таким образом, в статье была представлена адаптация имеющихся математических моделей распространения многоходовых социоинженерных атак, позволяющая учитывать силу информационного влияния. Полученная модель основывается на модели расчёта влияния агента и модели многоходовой социоинженерной атаки. Отметим, что математическая модель распространения многоходовых социоинженерных атак впервые

рассматривается в совокупности с моделью расчёта влияния агентов. Настоящее исследование находит своё применение при анализе социального графа сотрудников организации и опосредовано даёт возможность принимать таргетированные решения по повышению уровня защищённости организации от социоинженерных атак. В дальнейшем для улучшения полученной модели могут быть использованы подходы, применяемые к оценке интенсивности поведения пользователей [16], а именно использование байесовский сети доверия в контексте оценки интенсивности взаимодействия между пользователями.

Список литературы

[1] 2020 Cyber Security Statistics The Ultimate List Of Stats, Data & Trends [Электронный ресурс] URL: https://purplesec.us/resources/cyber-security-statistics/ (дата обращения: 26.01.2021)

[2] 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. Pp. 7152–7169.

[3] Naidoo R. A multi-level influence model of COVID-19 themed cybercrime // European Journal of Information Systems. 2020. Vol. 29. №3. Pp. 306–321.

[4] Social Engineering: How the new Work from Home concept has impacted the world [Электронный ресурс] URL: https://connect.geant.org/2020/10/02/social-engineering-how-the-new-work-from-home-concept-has-impacted-the-world (дата обращения: 16.02.2021)

[5] Exploiting a crisis: How cybercriminals behaved during the outbreak [Электронный ресурс] URL: https://www.microsoft.com/security/blog/2020/06/16/exploiting-a-crisis-how-cybercriminals-behaved-during-the-outbreak/ (дата обращения: 27.01.2021)

[6] 34 infosec experts discuss how to prevent the most common social engineering attacks [Электронный ресурс] URL: https://digitalguardian.com/blog/social-engineering-attacks-common-techniques-how-prevent-attack (дата обращения: 19.02.2021)

[7] Aldawood H., Skinner G. Analysis and Findings of Social Engineering Industry Experts Explorative Interviews: Perspectives on Measures, Tools, and Solutions // IEEE Access. 2020. Vol. 8. Pp. 67321–67329.

[8] Edwards M., Larson R., Green B., Rashid A., Baron A. (2017). Panning for gold: Automatically analysing online social engineering attack surfaces. computers & security. Vol. 69. Pp. 18–34.

[9] Steinmetz K.F. The Identification of a Model Victim for Social Engineering: A Qualitative Analysis // Victims & Offenders. 2020. Pp. 1–25.

[10] Абрамов М.В., Тулупьева Т.В., Тулупьев А.Л. Социоинженерные атаки: социальные сети и оценки защищенности пользователей. СПб.: ГУАП, 2018. 266 с.

[11] Chkhartishvili A.G., Gubanov D.A. Analysis of user influence types in online social networks: an example of VKontakte // In 2017 IEEE 11th International Conference on Application of Information and Communication Technologies (AICT). Pp. 1–3. IEEE

[12] Chkhartishvili A., Gubanov D. On Approaches to Identifying Information Spread Channels in Online Social Networks // 2019 Twelfth International Conference" Management of large-scale system development"(MLSD). IEEE, 2019. Pp. 1–4.

[13] Gubanov D. A Study of Formalizations of User Influence in Actional Model // 2020 13th International Conference" Management of large-scale system development"(MLSD). IEEE, 2020. Pp. 1–5.

[14] Khlobystova A.O., Abramov M.V., Tulupyev A.L., Zolotin A.A. Identifying the most critical trajectory of the spread of a social engineering attack between two users. // Informatsionno-upravliaiushchie sistemy [Information and Control Systems], 2018, № 6, Pp. 74–81. doi:10.31799/1684-8853-2018-6-74-81

[15] Khlobystova A.O., Tulupyeva T.V., Maksimov A.G., Korepanova A.A. An approach to quantification of relationship types between users based on the frequency of combinations of non-numeric evaluations. // In: Kovalev S., Tarassov V., Snasel V., Sukhanov A. (eds) Proceedings of the Fourth International Scientific Conference “Intelligent Information Technologies for Industry” (IITI’19). IITI 2019. Advances in Intelligent Systems and Computing, vol 1156, pp. 206-213. Springer, Cham. DOI: 10.1007/978-3-030-50097-9_21

[16] Toropova A.V., Tulupyeva T.V. Bayesian BeliefNetwork as a Behavior Intensity Rate Model on the Example of Posting in a Social Network //2020 XXIII International Conference on Soft Computing and Measurements (SCM). IEEE, 2020. Pp. 22–24.