DOI 10.37882/2500-3682.2025.08.01

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ: СОЦИАЛЬНО-ПСИХОЛОГИЧЕСКИЙ ФЕНОМЕН СОВРЕМЕННОСТИ

Бузыканова Екатерина Вячеславовна
Аспирант, Московский государственный университет имени М.В. Ломоносова
kate.buzykanova@yandex.ru

Аннотация: Социальная инженерия — это совокупность методов воздействия, основанных на использовании уязвимых мест человеческой психики. Ее суть заключается в использовании различных техник и манипуляций с целью получения ценной информации и ресурсов. В современном мире информационные технологии развиваются огромными темпами, именно поэтому возрастает значение социальной инженерии, используемого в том числе в рамках киберпреступности. Понимание механизмов воздействия человека и способов защиты от подобных атак становится одним из ключевых аспектов обеспечения информационной безопасности. Данная статья посвящена изучению междисциплинарного феномена с психологической точки зрения, рассмотрению его характерных особенностей.

Ключевые слова: социальная инженерия, киберпсихология, кибербезопасность, манипуляция, психология влияния.

SOCIAL ENGINEERING: A SOCIO-PSYCHOLOGICAL PHENOMENON OF MODERNITY

E. Buzykanova

Summary: Social engineering is a set of methods of influence based on exploiting the vulnerabilities of the human psyche. Its essence lies in the use of various techniques and manipulations to obtain valuable information and resources. In the modern world, information technology is developing at a tremendous pace, which is why the importance of social engineering, including as one of the methods of cybercrime, is increasing. Understanding the mechanisms of human impact and ways to protect against such attacks is becoming one of the key aspects of ensuring information security. This article is devoted to the study of an interdisciplinary phenomenon from a psychological point of view, considering the features of a set of methods.

Keywords: social engineering, cyber psychology, cybersecurity, manipulation, psychology of influence.

Впервые словосочетание «социальный инженер» было употреблено британским экономистом Дж. Греем в 1842 году в труде под названием «Верное средство против бедствий народов» в значении группы людей, знающих, как исправить существующие проблемы общества. Изначально термин «социальная инженерия» употреблялся в контексте экономики, философии, прикладной социологии такими деятелями как Т. Веблен, Джейн Аддамс, Дж. С. Дэвис, Р. Паунд, С. и Б. Веббы, М. Истмен, К. Поппер и др. [7; 18].

Как можно заметить, рассматриваемое нами понятие приобрело несколько иное значение нежели в классической социологии. В 1984 году в издании «2600: Ежеквартальный журнал "Хакер"» некий аноним выпустил статью, посвященную фрикингу, в которой употребил термин «социальная инженерия» в значении убеждения кого-либо выдать некоторую информацию. После этого понятие периодически стало появляться в журналах, связанных с хакерством, именно в данном значении [7]. Согласно Оксфордскому словарю, термин «социальная инженерия» («social engineering») имеет два различных толкования:

1. «попытка изменить общество и решить социальные проблемы в соответствии с определенными политическими убеждениями, например, путем изменения закона»;
2. «акт намеренного принуждения кого-либо поверить во что-то, что не является правдой, с целью предоставления личной информации, которая может быть использована для его обмана (используется в связи с компьютерной безопасностью) [13].

В современном поле понятие определяют поразному. Феномен является междисциплинарным предметом и исследуется в различных областях научного знания, таких как социология, экономика, юриспруденция, криминалистика, психология, компьютерные науки. Некоторые авторы указывают, что социальная инженерия – это искусство заставлять других делать то, что нужно тебе, искусство добычи конфиденциальной информации [10; 17]. Т. Грининг определяет термин как «метод получения паролей с помощью социальных механизмов» [5]. Социальная инженерия подразумевает механизмы манипулирования, психологического давления на человека, поиска его слабостей для сбора информации [2; 20]. В. Суворова и Л. Суворова выделяют три характеристики социальной инженерии: использование компьютерных технологий, стремление получить информацию, влия-

ние на уязвимые места в психике человека [21].

Таким образом, дадим обобщенное определение понятию «социальная инженерия». Социальная инженерия – совокупность методов получения информации преимущественно с использованием компьютерных технологий посредством преднамеренного психологического воздействия на уязвимости личности.

Социальная инженерия как совокупность методов

Существует множество способов установления контактов социальных инженеров с человеком. Электронная почта, социальные сети, мобильная связь, различные сайты, облачные сервисы – одни из наиболее популярных каналов воздействия [9].

Социальная инженерия как метод реализуется в нескольких последовательных этапах. К. Митник описал так называемый цикл атаки социальной инженерии, являющийся наиболее распространенной моделью. Цикл состоит из 4-х стадий:

1. исследование: сбор всей необходимой информации о человеке (объекте атаки);
2. создание раппорта и обретение доверия: может быть осуществлено с помощью упоминаний знакомых лиц, конфиденциальной информации и т. д.;
3. пользование доверием: просьба выполнить необходимое инженеру действие, манипулирование человеком;
4. использование: получение желаемого [17].

С внедрением инноваций в компьютерных областях наиболее уязвимым звеном в обмене информацией становится человек. Социальные инженеры используют различные техники воздействия ради совершения хищения в своих интересах [8; 19; 22]. Ниамсурен и Чой были одними из первых, кто указал на критически важную роль человека в защите информации. По их мнению, фокус исключительно на техническом аспекте не является достаточным для гарантирования безопасности [11]. На данный момент исследователи выделяют два основных типа социальной инженерии: «технологический взлом» и «атака на человека». «Технологический взлом» подразумевает обман через создание ложных представлений об интеракции с компьютерными ресурсами, к примеру, получение доступа к серверу посредством активации жертвой фишинговой ссылки. «Атака на человека» строится на межличностном взаимодействии инженера с объектом атаки и включает в себя различные манипулятивные техники [1; 4].

Важно уточнить, что некоторые техники социальной инженерии помимо злоумышленников используют люди разных профессий: «белые» хакеры, шпионы, HR-специалисты, специалисты по продажам, юристы, управленцы и даже психологи [6]. Более того, существует определенная этика при использовании методов не в деструктивных целях, основанная на максимально, насколько это возможно, уважительном отношении к человеку и соблюдении законов [15].

Существуют разные виды осуществления социальной инженерии с технической точки зрения. В современной криминалистике выделяют следующие как основные:

1. Фишинг (с англ. «ловля рыбы») – распространение вредоносных ссылок или вложений якобы доверенным лицом или организацией. Является одним из первых появившихся методов и до сих пор несет наибольшую угрозу безопасности.
2. Претекстинг – воздействие на объект по четкому заранее спланированному алгоритму из небольших последовательных шагов. Зачастую осуществляется с использованием мобильных звонков.
3. Троянский конь – автоматически устанавливаемое вредоносное приложение после открытия безобидных на первый взгляд файлов или приложений.
4. «Quid pro quo» (услуга за услугу) – вымогание информации/активов в обмен на осуществление услуги либо ради мнимой благой цели.
5. Вишинг – разновидность фишинга с использованием голосовой коммуникации с объектом (звонок или голосовое сообщение).
6. «Дорожное яблоко» или приманка – подбрасывание информационного накопителя с вредоносной программой сотрудникам компании под видом интересующей их информации [19; 22; 24].

Кроме вышеперечисленных методов социальные инженеры используют множество других способов получения данных. М. Янгаева также выделяет такие техники, как «вымогатель», то есть зашифровку важной информации с целью требования выкупа, и обратную социальную инженерию, смыслом которой является создание ситуации для добровольного обращения человека к социальным инженерам [24]. Дж. Грей отмечает вейлинг, означающий фишинг высокопоставленных членов организации, и анализ содержимого мусорных баков компании в качестве не менее эффективных методов сбора информации [15]. К. Кромбольц и коллеги среди иных техник социальной инженерии выделяют «серфинг через плечо», подразумевающий получение необходимых данных путем подглядывания в экран, байтинг, то есть размещение интересующих человека вредоносных ссылок на видном месте или в виде всплывающих окон, создание фейковых профилей, мобильных приложений, рассылку спам-сообщений [9].

Психологические особенности феномена социальной инженерии

Психология влияния играет ключевую роль в использовании метода социальной инженерии. Р. Чалдини выделил 6 фундаментальных принципов социального поведения, которые в той или иной ситуации подталкивают человека принять определенное решение:

1. Принцип последовательности – взяв на себя некоторое обязательство, человеку трудно от него отказаться, поскольку оно представляет из себя определенную точку опоры.
2. Принцип социального доказательства – подражание другим является одним из способом побороть неуверенность в собственных действиях за счет следования принципу сходства.
3. Принцип взаимного обмена – человек старается «отплатить» за предоставленное другим, а также предоставить некую компенсацию, прежде чем что-то приобрести.
4. Принцип дефицита – наименьшая доступность несет наибольшую ценность.
5. Принцип авторитета – людям свойственно подчиняться, кроме того, существует некий автоматизм реагировать на символы авторитета (статус).
6. Принцип благорасположения – склонность соглашаться со знакомыми и с привлекательными людьми.

Личный материальный интерес автор рассматривает как аксиому. Кроме того, уже тогда автор акцентирует внимание на ежедневном поступлении значительного массива информации, что сокращает внимательность и, как следствие, время на принятие решения [23].

М. Безиденаут и коллеги выделяют 7 уязвимостей, на которые воздействует социальный инженер, чтобы добиться желаемого результата: вызов сильного аффекта, когнитивная перегрузка, взаимность (теория социального обмена), построение взаимоотношений, диффузия ответственности и взывание к моральному долгу, влияние авторитета, стремление довести дело до конца и последовательность в деятельности. Однако авторы подчеркивают, что процесс принятия решения является комплексным многофакторным феноменом с уникальной реализацией. В рамках теории субъективной ожидаемой полезности, предложенной Л. Сэвиджем, люди склонны полноценно оценивать риски и вероятные выгоды перед вынесением окончательного решения, опираясь не только на существующую систему ценностей, но и на ситуационные факторы. В ситуации ограниченного времени некоторым людям особенно трудно принять самостоятельное взвешенное решение, что делает их уязвимыми перед социальным инженером [2]. Другие исследователи также отмечают, что податливости объекта социальной инженерии способствует авторитет инженера, личная симпатия, ощущение дефицита или уникальности предложения, постоянство и последовательность в действиях, ощущение взаимности, социально валидная просьба инженера [3; 10; 14].

Социальные инженеры широко используют различные манипуляции для достижения своих целей. По мнению К. Хэднеги любые манипуляции в социальной инженерии могут быть как негативными, то есть ведущими к ухудшению состояния объекта и оставления его в нем, так и позитивными, когда объект может с помощью инженера или самостоятельно справиться с последствиями атаки (например, зачастую родители так воздействуют на своих детей). Манипулирование сводится к следующим процессам:

1. Повышение уровня внушаемости объекта, например, с помощью НЛП, научения (формирование связи между внешним стимулом и желаемой эмоцией объекта), использования невербальных характеристик (определенные позы, цвета в одежде и т. д.), многократного повторения одной и той же идеи, введения в состояние стресса или возбуждения.
2. Контроль окружающей объект среды за счет изменения его окружения или воздействия на саму обстановку.
3. Принуждение пересмотреть ценности заключается в убеждении жертвы усомниться в собственных взглядах. Социальные инженеры используют технику как ловушку, окружая подобные просьбы или утверждения нейтральными и безобидными. Данная техника может иметь крайне негативные последствия, часто используется сектами для привлечения жертв в культ.
4. Внушение беспомощности за счет властного поведения или создания иллюзии острой нужды/дефицита времени.
5. Унижения и внушение чувства вины, которые объект будет пытаться преодолеть для возвращения своей репутации и повышения значимости в глазах социального инженера.
6. Запугивание объекта негативными последствиями, угрожающим видом [6].

Социальная инженерия использует такие практические направления психологии, как нейролингвистическое программирование (НЛП), трансактный и скриптовый анализы. Трансактный и скриптовый (сценарный) анализы были предложены психологом Э. Берном и часто используются специалистами в области убеждения. С помощью техник трансактного анализа социальные инженеры устанавливают параллельные трансакции с объ-

ектом, погружающие его в нужное состояние (например, в позицию ребенка, которому сложно сопротивляться родителю). Техники сценарного перепрограммирования выступают средством вскрытия или навязывания объекту определенных установок, помогающих им управлять [16]. Нейролингвистическое программирование было разработано Р. Бандлером и Дж. Гриндером в 1970-х годах как модель психотерапии. Далее НЛП стало широко использоваться в иных областях практической направленности, в том числе в социальной инженерии, как эффективный способ влияния на человека. Техника подстройки, техника якорения, определенная лексика, построение фразы, паравербальные характеристики – все это помогает социальному инженеру добиться желаемого [6; 16].

Выводы

Социальная инженерия – комплексный метод коммуникации, граничащий с искусством, используемый для влияния на человека с целью получения желаемого, будь то информация, действие или какой-либо объект. Социальные инженеры используют множество различных техник, как в сфере компьютерных технологий, так и психологического плана. В современной реальности данный феномен имеет мультидисциплинарный контекст, осложняющийся его использованием во множестве сфер, как бытовых, профессиональных, так и криминальных. Профилактика и предотвращение подобных правонарушений видится важным направлением развития научного и практического знания разных областей науки, в том числе психологии.

ЛИТЕРАТУРА

1. Abass I. Social Engineering Threat and Defense: A Literature Survey // Journal of Information Security, 2008. V. 9. Pp. 257-264.
2. Bezuidenhout M., Mouton F., Venter H. S. Social engineering attack detection model: SEADM // Information Security for South Africa, 2010. Pp. 1-8.
3. Bullée J.-WH., Montoya L., Pieters W., Junger M., Hartel P. On the anatomy of social engineering attacks – A literature-based dissection of successful attacks // J. Investig. Psychol. Offender Profil., 2018. V. 15. Pp. 20–45.
4. Foozy F. M., Ahmad R., Abdollah M. F., Yusof R., Mas'ud M. Z. Generic taxonomy of social engineering attack // Malaysian Technical Universities International Conference on Engineering & Technology, 2011. Pp. 1-7.
5. Greening, T. Ask and ye shall receive: a study in "social engineering" // SIGSAC Rev., 1996. V. 14(2). Pp. 8–14.
6. Hadnagy C., Wilson P. Social Engineering: The Art of Human Hacking. John Wiley & Sons, 2010. 416 p.
7. Hatfield J. M., Social engineering in cybersecurity: The evolution of a concept // Computers & Security, 2018. V. 73. Pp. 102-113.
8. Huber M., Kowalski S., Nohlberg M., Tjoa S. Towards Automating Social Engineering Using Social Networking Sites // 12th IEEE International Conference on Computational Science and Engineering, 2009. V. 3. Pp. 117-124.
9. Krombholz K., Hobel H., Huber M., Weippl E. Advanced social engineering attacks // Journal of Information Security and Applications, 2015. V. 22. Pp. 113-122.
10. Mouton F., Leenen L., Venter H.S. Social engineering attack examples, templates and scenarios // Computers & Security, 2016. V. 59. Pp. 186-209.
11. Nyamsuren E., Choi H.-J. Preventing Social Engineering in Ubiquitous Environment // Future Generation Communication and Networking, 2007. Pp. 573-577.
12. Orth M. For Whom Ma Bell Tolls Not [Электронный ресурс] / Los Angeles Times, October 1971. Режим доступа: http://historyofphonephreaking.org/docs/orth1971.pdf.
13. Social engineering [Электронный ресурс]. Oxford Learner's Dictionaries, 2024. Режим доступа: https://clck.ru/3F9mdA.
14. Uebelacker, S., Quiel, S. The Social Engineering Personality Framework // Workshop on Socio-Technical Aspects in Security and Trust, 2014. Pp. 24-30. doi: 10.1109/STAST.2014.12.
15. Грей Дж. Социальная инженерия и этичный хакинг на практике. / Пер. с англ. В.С. Яценкова. М.: ДМК Пресс, 2023. 226 с.: ил.
16. Кузнецов М.В. Социальная инженерия и социальные хакеры. БХВ-Петербург, 2007. 368 С.
17. Митник К., Саймон В. Искусство обмана. / Пер. с англ.: А. Груздев, А. Семенов. Компания АйТи, 2004. 360 с.
18. Поппер К. Открытое общество и его враги. Т. 1: Чары Платона / Пер. с англ. под ред. В.Н. Садовского. М.: Феникс, Международный фонд «Культурная инициатива», 1992. 448 с.
19. Сиротин В.П., Архипова М.Ю., Куликова С.В. и др. Социальная инженерия и информационная безопасность / Москва: Общество с ограниченной ответственностью "Эдитус", 2023. 264 с.
20. Старостенко Н., Старостенко О. Криминалистическая характеристика способов мошенничества, совершенного с использованием методов социальной инженерии // Проблемы правовой и технической защиты информации, 2020. № 8. С. 107-110.
21. Суворова В.В. Совершение преступлений с использованием социальной инженерии: постановка проблемы / В.В. Суворова, Л.А. Суворова // Теория и практика приоритетных научных исследований: сборник научных трудов по материалам VIII Международной научно-практической конференции, Смоленск, 13 августа 2019 года. – Смоленск: МНИЦ «Наукосфера», 2019. – С. 71-74.
22. Унукович А.С. Социальная инженерия и кибербезопасноть: виктимологический аспект // Психопедагогика в правоохранительных органах, 2021. №3 (86).
23. Чалдини Р. Психология влияния / Пер. с англ.: Е. Волкова, И. Волкова. СПб: Издательство «Питер», 2000. 271 с.: ил.

24. Янгаева М.О. Социальная инженерия как способ совершения киберпреступлений // Вестник Сибирского юридического института МВД России, 2021. №1 (42). С. 133-138.