Секция «Психология цифрового мира»

Социальная инженерия: вызов современности

Научный руководитель – Солдатова Галина Владимировна

Бузыканова Екатерина Вячеславовна

Аспирант

Московский государственный университет имени М.В.Ломоносова, Факультет психологии, Кафедра психологии личности, Москва, Россия

E-mail: frant1900@gmail.com

Одной из наиболее актуальных тем современности является кибермошенничество, наносящее колоссальный ущерб как гражданам, так и компаниям государств разных стран. В связи с высокой значимостью данной темы в практическом поле все больше ученых уделяют внимание ее исследованию. Кибермошенничество изучается в рамках множества дисциплин, включая экономику, юриспруденцию, социологию, психологию и др. Несмотря на совершенствование различных способов защиты информации, именно человек остается самым уязвимым звеном в процессе ее обмена [9].

Социальная инженерия – один из ключевых методов воздействия на человека с целью получения желаемой информации. Феномен лежит на острие множества дисциплин. На текущий момент ни в практическом, ни в научном поле не существует единого определения феномена. Родоначальником понятия является К. Митник, известный хакер, определивший соц. инженерию как искусство заставлять людей делать что-либо для них специфичное [2]. В юридической сфере социальная инженерия подразумевает преступление в сфере компьютерной безопасности с целью получения информации путем использования слабых мест в психике человека [4, с. 135]. С точки зрения компьютерной безопасности феномен можно охарактеризовать, по аналогии с определением К. Митника, как некоторое искусство принуждения человека компрометировать информационные системы [10]. В психологическом поле существует несколько подходов к определению понятия. Общим знаменателем служат следующие характеристики:

· метод психологического воздействия на человека;

· имеет определенную цель в виде принуждения человека;

· итоговой целью служит конфиденциальная информация либо некие конкретные действия со стороны жертвы [1; 6; 11].

Существующие психологические исследования в области социальной инженерии опираются на Р. Чалдини, описавшего шесть основополагающих принципов поведения человека. Седьмой принцип в значении желания обретения как можно больших благ автор вынес как аксиому. Данные принципы были подтверждены М. Безиденаут, Ф. Мутон, Дж. Буле и коллегами в качестве фундамента для психотехник, лежащих в основе влияния социальных инженеров на человека [6; 11; 13].

Исследователи указывают на два ключевых типа воздействия на человека: «атака на человека» и «технологический взлом» [5; 7]. Среди конкретных техник, выступающих средством сбора информации, выделяются фишинг, использование фейковых сайтов, аккаунтов в социальных сетях, «quid pro quo», лжеантивирус, троянский конь, байтинг, претекстинг и др. [3; 4; 10].

Отличительной особенностью использования социальной инженерии выступает множество манипулятивных техник. С. Hadanegy, один из ведущих специалистов в данной сфере, отмечает крайнюю значимость манипулятивных техник в воздействии на человека. Среди основных категорий автор перечисляет влияние на внушаемость человека, в том

числе с помощью нейролингвистического программирования, внушение состояния беспомощности, манипуляцию чувством вины, подрыв ценностной картины мира, запугивание и др. [8].

Реализация социальной инженерии заключается в нескольких ключевых этапах, впервые описанных К. Митником. Цикл атаки состоит из четырех этапов: сбор информации, установление раппорта, манипуляция, получение желаемой информацией [2]. Современные исследования детализируют описанный выше процесс, подчеркивая важность подробной проработки плана атаки, определения цели, коммуникативных навыков инженера [12].

В настоящее время кибермошенничество представляет серьезную угрозу благополучия как отдельных граждан, так и компаний, и целых государств. Считаем важным обозначить ключевую роль человека как наиболее незащищенного звена в цепи передачи информации, в связи с чем именно с точки зрения научного знания представляется целесообразным описать существующие механизмы влияния, особенности уязвимости личности перед лицом социальных инженеров, а также, в рамках будущих исследований, способы профилактирования и противодействия всевозможным техникам социальной инженерии.

Источники и литература

1) Грей Дж. Социальная инженерия и этичный хакинг на практике / Пер. с англ. В. С. Яценкова. – М.: ДМК Пресс, 2023. – 226 с.: ил.
2) Митник К., Саймон В. Искусство обмана / Пер. с англ.: А. Груздев, А. Семенов. – Компания АйТи, 2004. – 360 с.
3) Социальная инженерия и информационная безопасность / В. П. Сиротин, М. Ю. Архипова, С. В. Куликова и др. – М.: Общество с ограниченной ответственностью "Эдитус", 2023. – 264 с.
4) Янгаева М. О. Социальная инженерия как способ совершения киберпреступлений // Вестник Сибирского юридического института МВД России, 2021. — №1 (42). — С. 133-138.
5) Abass, I. Social Engineering Threat and Defense: A Literature Survey // Journal of Information Security, 2008. — V. 9. — Pp. 257-264. — doi:10.4236/jis.2018.94018.
6) Bezuidenhout M., Mouton F., Venter H. S. Social engineering attack detection model: SEADM // Information Security for South Africa, Johannesburg, South Africa, 2-4 Aug. – 2010. – URL: https://ieeexplore.ieee.org/document/5588500 (accessed 12.11.2024).
7) 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.
8) Hadnagy C., Wilson P. Social Engineering: The Art of Human Hacking. – IN.: John Wiley & Sons, 2010. – 416 p.
9) Nyamsuren, E., & Choi, H.-J. Preventing Social Engineering in Ubiquitous Environment // Future Generation Communication and Networking, 2007. — Pp. 573-577. — doi:10.1109/fgcn.2007.185.
10) Krombholz K., Hobel H., Huber M., Weippl E. Advanced social engineering attacks // Journal of Information Security and Applications. – 2015. – V. 22. – P. 113-122. – URL: https://doi.org/10.1016/j.jisa.2014.09.005 (published: 09.07.2015).
11) Mouton F., Leenen L., Venter H.S. Social engineering attack examples, templates and scenarios // Computers & Security, 2016. – V. 59. – P. 186-209. – URL: https://doi.org/10.1016/j.cose.2016.03.004 (published: 29.03.2016).

12) Mouton F., Malan M. M., Leenen L., Venter H. S. Social engineering attack framework // Information Security for South Africa, 2014. — Pp. 1-9. — doi:10.1109/ISSA.2014.6950510.

13) On the anatomy of social engineering attacks – A literature-based dissection of successful attacks / Bullée J.-WH., Montoya L., Pieters W. et al. // Journal of Investigative Psychology and Offender Profiling. – 2018. – V. 15, I. 1. – P. 20–45. – URL: https://doi.org/10.1002/jip.1482 (published: 14.07.2017).