9. Киберугрозы финансовой отрасли: промежуточные итоги 2023 года [Электронный ресурс]. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/financial-industry-security-interim-2023/

10.Мифы и реальность технологий кибериммунитета [Электронный ресурс]. – URL: https://blog.kaspersky.kz/cyberimmunity-technology-myths/27161/

11. Centerm будет предустанавливать Kaspersky Thin Client на свою аппаратную платформу [Электронный ресурс]. – URL: https://os.kaspersky.ru/latest/kaspersky-and-centerm-to-provide-cyber-immune-thin-clients-worldwide/

12. «Лаборатория Касперского» и TSplus подписали соглашение о партнерстве [Электронный ресурс]. – URL: https://os.kaspersky.ru/latest/kaspersky-and-tsplus-sign-a-partnership-agreement/

13. «Лаборатория Касперского» и «ИнфоТеКС» продолжат развивать технологическое партнерство [Электронный ресурс]. – URL: https://www.kaspersky.ru/about/press-releases/2023_laboratoriya-kasperskogo-i-infoteks-prodolzhat-razvivat-tehnologicheskoe-partnyorstvo

14. «Лаборатория Касперского» и «Систэм Электрик» планируют создавать кибериммунные устройства на основе KasperskyOS для промышленных и энергетических предприятий [Электронный ресурс]. – URL: https://finance.rambler.ru/business/51006506-laboratoriya-kasperskogo-i-sistem-elektrik-planiruyut-sozdavat-kiberimmunnye-ustroystva-na-osnove-kasperskyos-dlya-promyshlennyh-i-energeticheskih-predpriyatiy/

15. Кибериммунитет обретает реальные очертания [Электронный ресурс]. – URL: https://www.anti-malware.ru/analytics/Technology_Analysis/Cyber-Immunity

16. The IBM Security Immune System. [Электронный ресурс]. – URL: https://onwireco.com/the-ibm-security-immune-system/

17. The Power of the Security Immune System [Электронный ресурс]. – URL: https://securityintelligence.com/the-power-of-the-security-immune-system/

18. Integrated, End-To-End Cybersecurity Strategy [Электронный ресурс]. – URL: https://www.siainnovations.com/blog/integrated-end-to-end-cybersecurity-strategy/

Ю. М. Графова,
аспирант,
Казанский инновационный университет
имени В. Г. Тимирясова

НЕКОТОРЫЕ МЕРЫ ПРОТИВОДЕЙСТВИЯ СОЦИОИНЖЕНЕРНЫМ АТАКАМ

Аннотация. В работе рассматриваются образовательно-просветительские меры противодействия социоинженерным атакам. Отмечается, что обучение сотрудников компании методам противодействия социоинженерным атакам является наиболее эффективным средством защиты от такого типа угроз. Таким об-

разом, чем более четко обучаемые способны соотносить события на их рабочем месте с обучением, которое они получают, тем более вероятно, что они будут приводить в действие процедуры обеспечения безопасности.

Ключевые слова: социальная инженерия, мошенничество, образование, профилактика, просвещение

SOME MEASURES TO COUNTER SOCIOENGINEERING ATTACKS

Abstract. The paper considers educational and educational measures to counter socioengineering attacks. It is noted that training company employees in methods of countering socioengineering attacks is the most effective means of protection against this type of threat. Thus, the more clearly trainees are able to relate events in their workplace to the training they receive, the more likely they are to put safety procedures in place.

Keywords: social engineering, fraud, education, prevention, education

В основе развития социальной инженерии лежит несколько базовых идей. Эпистемологическая асимметрия возникает, когда человек или группа обладает значительным преимуществом в знаниях над другими людьми. Технократическое доминирование возникает, когда человек обладает высокой степенью технических знаний и использует эти знания для осуществления изменений в поведении других людей, когда такое поведение ставит жертву в подчинение злоумышленнику.

Телеологическая замена происходит, когда человек или группа замещает в другом индивидууме или группе первоначальную цель или цель их поведения со своими собственными, часто через изменение самого поведения цели. Эти свойства составляют основу социальной инженерии, выражается ли это в политике или киберпространстве. Все вышесказанное позволяет глубже понять характер потенциальных угроз.

Использование знаний в качестве контрмеры социоинженерным атакам требует, чтобы пользователь опирался на свои навыки в том, что такое угроза и как она действует, чтобы адекватно реагировать на нее, если она возникнет [1]. Именно по этой причине можно отметить, что лучший способ избежать участи жертвы атак социальной инженерии – быть осведомленным в вопросах противодействия таким атакам, т. е. в вопросах информационной безопасности.

Таким образом, чем более четко обучаемые способны соотносить события на их рабочем месте с обучением, которое они получают, тем более вероятно, что они будут приводить в действие процедуры обеспечения безопасности.

Корреляции такого рода включают в себя видение некоторых конкретных социоинженерных атак, с которыми сталкивается сотрудник, и использование их моделей в обучении. Так как особенности любой реальной атаки будут отличаться во многих важных отношениях из учебных примеров, необходимо отработать правильную реакцию, опирающуюся на способность обучаемого абстрагироваться от специфических особенностей атаки.

Необходимость проводить соответствующее обучение сотрудников для повышения у них навыка противостояния социоинженерным атакам отмечена и в работе Dina Aladawy, Kristian Beckers, Sebastian Pape [2]. Указанные авторы считают, что наиболее эффективными в данной области могут стать деловые игры, в процессе которых сотрудники учатся противостоять мошенникам. Соответственно, сегодня назрела острая необходимость обеспечить обучение сотрудников компаний умению распознавать риски, связанные с социоинженерными атаками, и противостоять им. Практика показывает, что осведомленность сотрудников о возможных угрозах является лучшей защитой от утечки данных [3].

Таким образом, можно констатировать, что обучение сотрудников компании методам противодействия социоинженерным атакам является наиболее эффективным средством защиты от такого типа угроз.

Список литературы

1. Sanders, C. A. (2018). *Social Engineering Knowledge Measured as a Security Countermeasure*. (Master's thesis). – URL: https://scholarcommons.sc.edu/etd/4567

2. Aladawy, D., Beckers, K., & Pape, S. (2018). PERSUADED: Fighting Social Engineering Attacks with a Serious Game. In *Lecture notes in computer science* (Pp. 103–118). – DOI: https://doi.org/10.1007/978-3-319-98385-1_8

3. Hussain Ali Aldawood, Geoffrey SkinnerA Critical Appraisal of Contemporary Cyber Security Social Engineering Solutions: Measures, Policies, Tools and Applications.

Г. А. Грищенко,
кандидат юридических наук, доцент,
Московский государственный юридический
университет имени О. Е. Кутафина (МГЮА)

ПРАВОВЫЕ ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЕТЕЙ В ЦИФРОВОЙ СРЕДЕ

Аннотация. В современном цифровом мире дети являются наиболее уязвимой аудиторией пользователей в сети Интернет. Чрезмерное доверие несовершеннолетних к популярным блогерам (инфлюенсерам) приводят к тому, что зачастую размываются границы реальной и виртуальной жизни, и, как следствие, может привести к причинению вреда жизни и (или) здоровью себе и окружающим. Целью статьи является проведение анализа законодательства, правоприменительной практики, общественного мнения и научной литературы в области регулирования информационной безопасности детей, и выработка рекомендаций по совершенствованию правовой регламентации соответствующих отношений с учетом новых вызовов и угроз в условиях цифровизации. Проведенный анализ показал недостаточность и неэффективность регулирования некоторых аспектов обеспечения информационной безопасности детей в цифровой среде. В качестве