УДК 336.71:004.056

DOI: 10.18572/1812-3945-2021-2-50-56

Социальная инженерия vs кибербезопасность в банковской сфере*

Казаченок Олеся Павловна,
доцент кафедры гражданского и международного частного права (базовая кафедра Южного научного центра Российской академии наук) Волгоградского государственного университета, кандидат юридических наук
o.kazachenok@yandex.ru

Kazachenok Olesya P.
Associate Professor of the Department of Civil and Private International Law (the Main Department of the Southern Research Center of the Russian Academy of Sciences) of the Volgograd State University PhD (Law)

В статье рассмотрено применение социальной инженерии как метода психологического воздействия на человека с целью получения доступа к конфиденциальной банковской информации в условиях цифровизации всех процессов в банковской сфере. Выявлены основные проблемы кибербезопасности на фоне применения преступниками совокупности психологических, социальных и технологических методов получения доступа к банковским данным. На фоне постоянного совершенствования технических мер кибербезопасности самым слабым звеном любой информационной системы становится человек, имеющий доступ к ней. Проанализированы способы незаконного получения банковской информации с применением приемов социальной инженерии, определены основные направления формирования системы защиты конфиденциальной банковской информации.

Ключевые слова: цифровизация, социальная инженерия, кибербезопасность, фишинг, проблемы кибербезопасности, кибератаки, киберпреступность, криптоджекинг.

* Исследование выполнено при финансовой поддержке Российского научного фонда (проект № 20-18-00314).

KAZACHENOK O.P. SOCIAL ENGINEERING VS CYBERSECURITY IN THE BANKING SPHERE

The article discusses the concept of social engineering as a method of psychological influence on a person in order to gain access to confidential information. The author draws attention to the fact that cybercrime cur-rently poses a serious threat not only to individuals, but also to banks. The main problems of cybersecurity are identified, which are primarily due to the fact that criminals are becoming more sophisticated not only in the use of technology, but also in psychology. Using specific examples, methods of deceiving people using social engineering techniques are an-alyzed. The author defines the main directions for the prevention of new crimes in the banking sector.

Keywords: digitalization, social engineering, cybersecurity, phishing, cybersecurity problems, cyberattacks, cybercrime, cryptojacking.