Criminological Analysis of Determinants of Cybercrime Technologies

Lola F. Tatarinova\textsuperscript{a}, Karimzhan N. Shakirov\textsuperscript{b} and Danila V. Tatarinov\textsuperscript{b}

\textsuperscript{a}"Turan" University, KAZAKHSTAN; \textsuperscript{b}Al-Farabi Kazakh National University, KAZAKHSTAN.

ABSTRACT
An important task, the government, particularly law enforcement officers and scientists, faces in the rapid development of information technologies, is to prevent crimes committed with their application. Comprehensive analysis of the criminological characteristics of computer crimes, which is the aim of this study, provides an opportunity to identify the motives of these crimes to determine the most effective ways to eliminate them, as well as to work out the best ways and investigation means of criminal cases in this category. One of the fundamental structural elements of the national security of any state in the period of cyberspace development is to protect all information resources and communication networks against criminal assault. A complete analysis of computer crimes requires the understanding of motivation of illegal intrusion into information systems in order to obtain the information, stored in them, as well as using the opportunities provided by these systems or disabling the whole system or its components. The statement above is confirmed by the global use of computer technologies, information and communication networks.

KEYWORDS
Criminology; cyber security; information technologies; cryptography; criminological methods

ARTICLE HISTORY
Received 15 September 2015
Revised 10 November 2015
Accepted 22 February 2016

Introduction
Cybersecurity is possible through the methods of criminology.

The innovation of the article is an attempt to adapt the methods of criminological analysis to cyberspace. K. Driscoll (2016) notes, that cyberspace is an integral part of the encrypted system. Thus, the knowledge of cryptography helps to identify and prevent cybercrimes.

An important tool for protection against computer crimes is cyberhygiene – the improvement of the Internet culture, an integral part of which is the possession of the complex procedures applied by cybercriminals. Many works are written on the "phishing" methodology (Murashbekov, 2015, Leukfeldt, 2015a, Leukfeldt, 2015b,

CORRESPONDENCE Danila V. Tatarinova \textsuperscript{a} danila_tatarinov@mail.ru
© 2016 Tatarinova, Shakirov and Tatarinov. Open Access terms of the Creative Commons Attribution 4.0 International License (http://creativecommons.org/licenses/by/4.0/) apply. The license permits unrestricted use, distribution, and reproduction in any medium, on the condition that users give exact credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if they made any changes.
Notes on contributors

Lola F. Tatarinova is PhD, Associate professor of Department of Jurisprudence and International Law, “Turan” University, Almaty, Kazakhstan.

Karimzhon N. Shakirov is Doctor of Jurisprudence, Professor of International Law, Al-Farabi Kazakh National University, Almaty, Kazakhstan.

Danila V. Tatarinov is PhD, Associate professor of International Law, Al-Farabi Kazakh National University, Almaty, Kazakhstan.

References


