

DOI: 10.18572/1812-3783-2021-7-61-64

ТРАНСФОРМАЦИЯ МЕХАНИЗМА СОВЕРШЕНИЯ ХИЩЕНИЙ С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ СОТОВОЙ СВЯЗИ: ПОСТАНОВКА ПРОБЛЕМЫ

Поддубный Илья Васильевич,
адъюнкт Орловского юридического института
Министерства внутренних дел Российской Федерации имени В.В. Лукьянова
wf0109@yandex.ru

В статье на основе анализа юридической литературы, статистических данных, материалов судебно-следственной практики, информации, размещенной в средствах массовой информации и сети Интернет, было проанализировано современное состояние и трансформация механизма дистанционных хищений, совершаемых с использованием средств сотовой связи. Изучены основные способы совершения хищений, применяемые при этом приемы и технологии. Автором сделан вывод о том, что преступность, связанная с дистанционными хищениями, совершаемыми с использованием средств сотовой связи, с каждым годом приобретает новые объемы, злоумышленники активно используют технологии и методы социальной инженерии, которые имеют персонифицированный характер.

Ключевые слова: дистанционное хищение, вишинг, социальная инженерия, сотовая связь, Интернет.

TRANSFORMATION OF THE MECHANISM OF EMBEZZLEMENT USING MOBILE COMMUNICATION DEVICES: PROBLEM SETTING

Poddubnyy Ilya V.
Junior Scientific Assistant of the Orel Law Institute of the Ministry of the Interior
of the Russian Federation Named after V.V. Lukyanov

In the article, based on the analysis of legal literature, statistical data, materials of forensic practice, information posted in the media and the Internet, the current state and transformation of crime in the field of remote theft committed using cellular communications were analyzed, the main methods were studied. committing theft, the techniques and technologies used. The author concludes that criminality associated with remote theft, committed using cellular communications, is gaining momentum every year. Attackers actively use technology and social engineering techniques, and their attacks are often directed at specific individuals who can be defined as "targeted".

Keywords: remote theft, vishing, social engineering, cellular communications, the Internet.