СИСТЕМА КРИМИНОЛОГИЧЕСКИХ И ПРАВОВЫХ МЕР ПРОТИВОДЕЙСТВИЯ МОШЕННИЧЕСТВУ В СЕТИ ИНТЕРНЕТ

Старостенко О.А., Старостенко Н.И.
Краснодарский университет МВД России, г. Краснодар
email: olegstaros94@gmail.com

Аннотация. Данная статья посвящена исследованию систем криминологических и правовых мер противодействия мошенничеству в сети Интернет. В статье, на основе изучения и анализа возникновения кибермошенничества, сформирована система мер противодействия рассматриваемому преступлению (меры разделены на криминологические и правовые); выделено два основных объекта познания в рамках исследования способа совершения кибермошенничества; в целях предупреждения кибермошенничества предложена Национальная Стратегия кибербезопасности. Данная стратегия должна быть направлена на следующие ключевые пункты:

- борьба с анонимностью;
- законотворческая деятельность в данной области;
- сотрудничество с иностранными государствами;
- обеспечение безопасности в киберпространстве;
- создание и внедрение новых правоохраниельных органов;
- повышение цифровой грамотности общества;
- создание инструкции по предупреждению виктимного поведения в Интернете.

Ключевые слова: криминология, кибермошенничество, информационно-телекоммуникационное мошенничество, противодействие, способ совершения, киберпространство, кибербезопасность, сотрудничество.

В настоящее время в России происходит становление нового – информационного общества, что характеризуется взрывным ростом и развитием сферы информационно-телекоммуникационных услуг. Количество пользователей смартфонами, планшетами, персональными компьютерами и ноутбуками выросло вдвое по сравнению с предыдущим годом [1].

Вследствие влияния и взаимодействия данных процессов, изменилась и преступность. Так, например, глобализация населения привела к возникновению такого негативного последствия, как мошенничество в сети Интернет. В настоящее время рассматриваемое преступление приобрело необратимый характер, мошенники стали практически неуловимы. На наш взгляд, это связано с колоссальным внедрением научно-технического прогресса в повседневную жизнь, который, по сути, и позволяет мошенникам реализовывать противоправные деяния.

Изучив и проанализировав возникновение кибермошенничества в России и соседних странах, нами сформирована система мер противодействия рассматриваемому преступлению:

- выявление, ослабление и нейтрализация причин онлайн-мошенничества;
- выявление мотивирующих факторов, побуждающих к совершению преступления;
- установление лиц, обладающих повышенным криминальным риском. Оказание воздействия с целью снижения установленного риска;
- установление лиц по психологическим факторам, указывающим на их способность совершать преступления и соответствующее корректирующее воздействие на них [2, с. 47-51].

Рассмотренные меры можно разделить по способу противодействия на криминологические и правовые. Первые направлены на противодействие основным

детерминантам кибермошенничества: анонимность, экстерриториальность, отсутствие знаний об информационной безопасности. В изучаемых мерах содержится ряд предложений и предписаний по профилактике и совершенствованию информационной безопасности и информационных технологий. Задача правовых мер – выдвижение и реализация предложений, направленных на совершенствование действующего законодательства об ответственности за совершение мошенничества в сфере информационно-телекоммуникационных технологий.

Нами предложено в исследовании способа совершения мошенничества в сфере информационно-телекоммуникационных технологий выделить два основных объекта познания, а именно: мошенничество, совершаемое путем воздействия на лицо, и мошенничество, совершаемое посредством воздействия на оборудование. Меры противодействия можно также разделить на социальные и технические. Сущность социальных заключается в их направленности на развитие информационной грамотности населения. Задача технических мер – внедрение информационных технологий в жизнь общества, анализ и разработка антишпионского и антивирусного программного обеспечения, борьба с анонимностью.

Как отмечает М.А. Простосердов, отсутствие четко определенных интернет-границ создает ряд трудностей в привлечении виновных к соответствующей ответственности, и единственное решение проблемы трансграничности киберпреступлений – международное сотрудничество [3, с. 174].

Проанализировав соглашения о сотрудничестве государств, нами установлено, что Россия принимает участие в международных сотрудничествах по борьбе с IT-мошенничеством. Однако такие сотрудничества выступают лишь первым этапом в противодействии рассматриваемому явлению, на котором устанавливаются основные правила противодействия.

М.А. Простосердов в своем диссертационном исследовании предлагает определить следующий этап противодействия преступлениям в сфере коммуникационных технологий – принятие Конвенции ООН, которая должна состоять из двух частей. В первой части он считает необходимым дать определение киберпреступлению и кибепространству. Во второй части – определить и установить систему мер противодействия трансграничному характеру кибепреступлений, определить основы международного сотрудничества. Мы считаем, что позиция автора имеет рационально зерно, но в нашем случае, имеется необходимость в понимании определения кибермошенничества и, соответственно, разработки мер противодействия искомому явлению. Также представляется, что положения предложенной Конвенции не должны нарушать независимость государств и их законные интересы, а меры противодействия должны защищать права и свободы граждан.

Основываясь на собранном эмпирическом материале и проведенном исследовании, можно сделать вывод, что отечественный законодатель не уделяет соответствующего внимания противодействию IT-мошенничеству. Некоторые существующие статьи УК РФ составлены некорректно и требуют срочного операционного вмешательства. Также мы считаем, что ввиду постоянного прогресса и появления новых понятий, необходимо согласовать с другими федеральными органами внесение изменений в Федеральный закон «Об информации, информационных технологий и защите информации»; законодательно закрепить определение кибермошенничества и кибепространства, распространив на него действие данного Федерального закона [4].

Говоря и криминологических мерах в России в целях предупреждения кибермошенничества, имеется необходимость в принятии Национальной Стратегии

кибербезопасности [5, с. 213]. Данная стратегия должна быть направлена на следующие ключевые пункты:

- борьба с анонимностью;
- законотворческая деятельность в данной области;
- сотрудничество с иностранными государствами;
- обеспечение безопасности в киберпространстве;
- создание и внедрение новых правоохраниельных органов;
- повышение цифровой грамотности общества;
- создание инструкции по предупреждению виктимного поведения в Интернете.

Библиографический список

1. Информационно-телекоммуникационные итоги года. [Электронный ресурс] // режим доступа: http://www.riocenter. ru/ru/events_and_analyst/ (дата обращения: 03.11.2020 г.)
2. Желудков М.А. Обоснование реализации системных защитных мер в механизме предупреждения корыстной преступности // Вестник Волгоградской академии МВД России. − 2014. − № 4 (31). – С. 47-51.
3. Простосердов М.А. «Экономические преступления, совершаемые в киберпространстве, и меры противодействия им». – 174 с.
4. Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (с изменениями и дополнениями) [Электронный ресурс] // режим доступа: http://base.garant.ru/12148555/#ixzz6coaEX1vC (дата обращения 04.11.2020г.).
5. Дремлюга Р.И. Интернет-преступность // Монография. – 213 с.

SYSTEM OF CRIMINOLOGICAL AND LEGAL MEASURES FOR COUNTERING FRAUD ON THE INTERNET

Starostenko O.A., Starostenko N.I.
Krasnodar University of the Ministry of Internal Affairs of Russia, Krasnodar
email: olegstaros94@gmail.com

Abstract. This article is devoted to the study of systems of criminological and legal measures to combat fraud on the Internet. In the article, based on the study and analysis of the occurrence of cyber fraud, a system of measures to counter the crime in question is formed; division of measures into criminological and legal; identified two main objects of knowledge in the study of the way of committing cyber fraud; in order to prevent cyber fraud, a National Cyber Security Strategy has been proposed. This strategy should focus on the following key points:

- fight against anonymity;
- legislative activity in this area;
- cooperation with foreign states;
- ensuring security in cyberspace;
- creation and implementation of new law enforcement agencies;
- increasing the digital literacy of society;
- creation of instructions for the prevention of victim behavior on the Internet.

Keywords: criminology, cyber fraud, information and telecommunications fraud, counteraction, method of committing, cyberspace, cyber security, cooperation.