5. Luneev V.V. (1980) Criminal behavior: motivation, forecasting, prevention: textbook [*Prestupnoe povedenie: motivaciya, prognozirovanie, profilaktika: uchebnoe posobie*]. - Moscow: Military University Publishing House. 137 p.

6. Rastoropova O.V. Nechaev A.D. (2017) Crimes of economic orientation: concept, signs, system // Gaps in Russian legislation. Legal Journal [*Prestupleniya ekonomicheskoj napravlennosti: ponyatie, priznaki, sistema // Probely v rossijskom zakonodatel'stve. YUridicheskij zhurnal*]. №2. p. 121-124.

7. Romanov V.V. (2017) Legal psychology: a textbook for an academic bachelor's degree [*Yuridicheskaya psikhologiya: uchebnik dlya akademicheskogo baccalaureate*]. Moscow: Yurayt Publishing House. 537 p.

8. Chernysheva E.V., Tyumentseva A.A. (2015) Motivation of criminal behavior in committing intentional crimes // Personality, family and society: questions of pedagogy and psychology [*Motivaciya prestupnogo povedeniya v sovershenii umyshlennyh prestuplenij // Lichnost', sem'ya i obshchestvo: voprosy pedagogiki i psihologii*]. №12 (57). Pp. 187-195.

9. Chankova E.V. (2014) Research of personal motivation // Theory and practice of social development [*Issledovanie motivacii lichnosti // Teoriya i praktika obshchestvennogo razvitiya*] №18. pp. 32-34.

10. Yuryeva V.G. (2016) Psychology of criminal behavior and its dependence on the accentuation of the criminal's character // Bulletin of the Taganrog Institute named after A.P. Chekhov [*Psihologiya prestupnogo povedeniya i ee zavisimost' ot akcentuacii haraktera prestupnika// Vestnik Taganrogskogo instituta imeni A.P. CHekhova*]. № 1. - 116-120.

УДК 159.9

ИСПОЛЬЗОВАНИЕ ПСИХОЛОГИЧЕСКОГО ВОЗДЕЙСТВИЯ ПРИ СОВЕРШЕНИИ МОШЕННИЧЕСТВА В УСЛОВИЯХ ЦИФРОВИЗАЦИИ ЭКОНОМИКИ

Н.В. Токарев

Аннотация. *В данной статье рассматриваются виды психологического воздействия при совершении мошенничества в условиях цифровизации экономики. Актуальность рассматриваемой проблемы обусловлена тем, что усложнение структуры финансового рынка и развитие системы электронных платежей привели к модернизации различных видов мошеннических схем и росту количества регистрируемых преступлений в сфере информационных технологий. Это связано с использованием технологических возможностей компьютерных систем для получения незаконной информации, возможностью сокрытия всех улик и сохранения анонимности в сети Интернет. В статье отмечено, что убытки от мошеннической деятельности имеют как финансовое проявление, так и социально-психологическое, включающее в себя ощущение разочарования, несправедливости, стресс. В результате анализа было выявлено, что данный вид обмана имеет две составляющие: технологическую и психологическую, которая воздействует на значимые элементы мотивации потенциальной жертвы и побуждает ее к совершению действий в интересах мошенников. К ним относятся стремление к получению прибыли («гарантированный доход –*

200%»), желание бесплатно или со значительной скидкой получить некоторые платные услуги и товары (неполучения оплаченного товара из online-магазинов), отзывчивость и жалость (мнимый сбор средств для приюта, помощь людям, попавшим в сложную жизненную ситуацию), страх («ваша карта заблокирована»). Стоит отметить, что на фоне высокого уровня тревожности наиболее часто влиянию мошенников поддаются люди старшего поколения, не всегда критически оценивающие ситуацию. На основании результатов исследования были предложены меры по борьбе с данным видом преступлений, включающие в себя как развитие национального и международного законодательства, так и проведение информационно-просветительской деятельности об угрозе со стороны мошенников, действующих в сети Интернет.

Ключевые слова: *информационные технологии, психологические аспекты, мошенничество, интернет-махинации, убеждение, криминальное манипулирование.*

THE USE OF PSYCHOLOGICAL INFLUENCE IN THE COMMISSION OF FRAUD IN THE CONTEXT OF THE DIGITALIZATION OF THE ECONOMY

N. Tokarev

Abstract. *This article discusses the types of psychological impact when committing fraud in the context of the digitalization of the economy. The relevance of the problem under consideration is due to the fact that the complexity of the financial market structure and the development of the electronic payment system have led to the modernization of various types of fraudulent schemes and an increase in the number of registered crimes in the field of information technology. This is due to the use of technological capabilities of computer systems to obtain illegal information, the possibility of hiding all evidence and maintaining anonymity on the Internet. The article notes that losses from fraudulent activities have both financial and socio-psychological manifestations, including feelings of frustration, injustice, and stress. As a result of the analysis, it was revealed that this type of deception has two components: technological and psychological, which affects the significant elements of the potential victim's motivation and encourages her to commit actions in the interests of fraudsters. These include the desire to make a profit ("guaranteed income-200%"), the desire to get some paid services and goods for free or at a significant discount (non-receipt of paid goods from online stores), responsiveness and pity (imaginary fundraising for a shelter, helping people who are in a difficult life situation), fear ("your card is blocked"). It is worth noting that against the background of a high level of anxiety, the most often influenced by scammers are people of the older generation, who do not always critically assess the situation. Based on the results of the study, measures were proposed to combat this type of crime, including both the development of national and international legislation, and the implementation of information and educational activities about the threat from fraudsters operating on the Internet.*

Keywords: *information technologies, psychological aspects, fraud, Internet fraud, persuasion, criminal manipulation.*

В современных условиях развития экономики информационные технологии все активнее начинают интегрироваться в жизнь общества, становятся его неотъемлемой

частью. Цифровизация помогает при решении множества задач, делает жизнь более комфортной. Благодаря ей произошли улучшения в банковской системе, появились новые продукты и online-услуги, а также усовершенствовались способы их оплаты. Однако, несмотря на все положительные стороны, усложнение структуры финансового рынка привело к модернизации различных видов мошеннических схем, что на данный момент является одной из глобальных проблем.

У продвинутых пользователей интернета есть все условия для того, чтобы совершить преступление, скрыть все улики и сохранить свою полную анонимность. По оценкам специалистов, от 85 до 97% преступлений в сети невозможно обнаружить, так как они имеют транснациональный характер [1].

По оценкам специалистов Главного управления экономической безопасности МВД России количество регистрируемых преступлений в сети и в IT сфере неуклонно растет. В условиях глобальной пандемии коронавирусной инфекции число случаев телефонного и интернет-мошенничества выросло на 76% по сравнению с первым полугодием 2019 года. На данный момент они занимают второе место от общего числа правонарушений. Более подробно это положение рассмотрено на рисунке 1 [2].

Убытки от мошеннической деятельности в Интернете имеют как финансовое проявление, так и социально-психологическое, включающее в себя ощущение разочарования, несправедливости, стресс. Именно поэтому данный вид обмана имеет две составляющие: технологическую и психологическую.

Знание психологии поведения человека даёт полный контроль мошенникам над выбранной целью, при совершении ими преступления в сети Интернет. Основными методами криминального манипулирования, также как и при совершении иных преступных деяний, являются убеждение и внушение.

В эпоху всеобщей цифровизации используются различные технологические возможности компьютерных систем, направленные на получение незаконной прибыли и информации. Основные виды мошенничеств в сети Интернет связаны с развитием системы электронных платежей, рынок которых ежегодно увеличивается примерно на 20% процентов, а вместе с этим растет число интернет-махинаций. Ежедневно жертвами сетевых мошенников становятся тысячи людей.

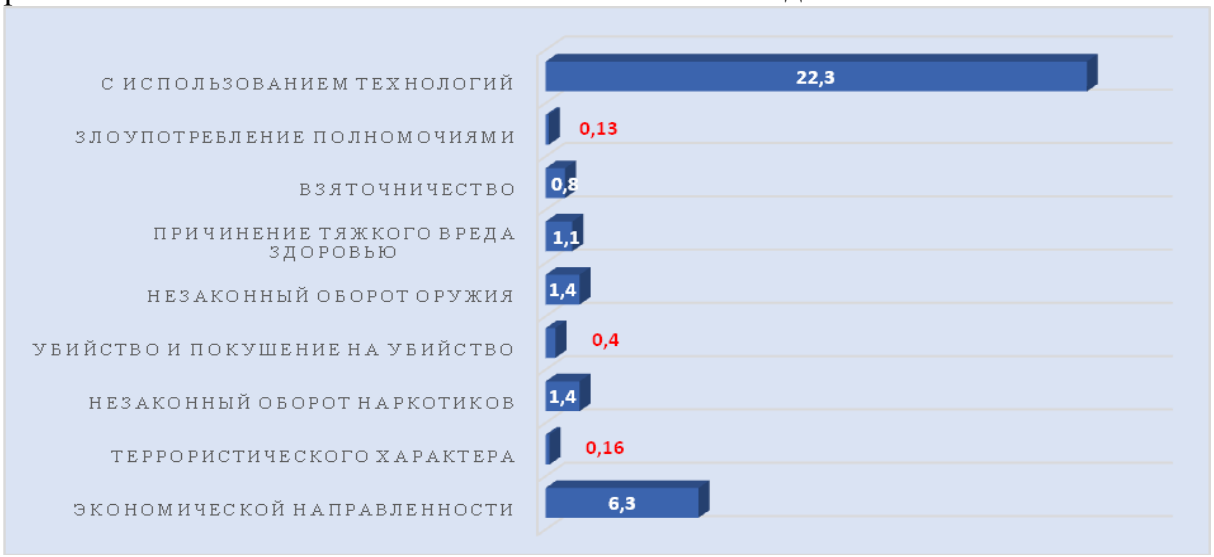

Рисунок 1 – Удельный вес отдельных видов преступлений от общего числа зарегистрированных преступлений, %

При совершении преступлений, связанных с использованием электронных платежей, мошенники опираются на чувства страха и паники потенциальных жертв. Часто возникают ситуации, когда населению поступают звонки от «банковских работников» для хищения денежных средств с расчетного счета под различными предлогами: «ваша карта заблокирована», «срочно оплатите счет», «ваш близкий человек попал в беду». Они достигают свою цель благодаря множеству ресурсов, к которым относятся информация (у преступников уже есть имя пользователя, адрес, номер телефона, банковские реквизиты), срочность, подмена телефона (на дисплее появляется официальный номер банка). На фоне высокого уровня тревожности многие поддаются влиянию мошенников, особенно люди старшего поколения, не всегда критически оценивающие ситуацию. Для того, чтобы защитить себя необходимо помнить, что никто из финансовых работников не будет предлагать решить какие-либо проблемы, узнавать номер или CVV-код без вашего личного присутствия [3].

В последнее время участились случаи неполучения оплаченного товара из online-магазинов. Для этого мошенники создают поддельные предприятия с хорошими отзывами и, используя их, начинают вступать в электронную платёжную систему на договорной основе. При совершении данного вида преступлений опираются на чувство корысти, жажду денег.

Этот вид психологического воздействия используется при рекламе запрещенных букмекеров, online-казино и Telegram-каналов, раздающих деньги. Они предлагают вкладывать средства без каких-либо рисков и со 100% выплатой. Отправляя всего 100 рублей, человек должен получить или выиграть 25000 рублей, однако вернуть назад свои денежные средства еще никому не удалось.

В развивающейся информационной эпохе большой спрос получило online общение, «социальные сети». Благодаря этому получил распространение самый ужасный вид интернет-мошенничества, связанный со спекуляцией на трагедии другого человека. В сети создают клон настоящего сайта благотворительной организации, меняют реквизиты для перечисления денег на свои или создают просто полностью новый вымышленный фонд с просьбой по сбору денег (пожертвований) для помощи больным. Аферисты пытаются играть на ваших чувствах доброты и сострадания, говорят, что нужна срочная операция, счёт идёт на считанные дни, если не помощь сейчас, то он или она умрёт.

Многообразие мошеннических схем в Интернете вызывает необходимость как национального, так и международного законодательного обеспечения борьбы с этим преступлением.

Для решения вышеперечисленных задач Федеральным законом от 29.11.2012 № 207-ФЗ была введена статья 159.6 УК РФ «Мошенничество в сфере компьютерной информации», включающая 4 пункта. Она посвящена хищению чужого имущества путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи информационно-телекоммуникационных сетей. За хищение имущества предусмотрены разные типы наказания – от штрафа до лишения свободы на несколько лет [4].

Серьезной задачей государственных органов, в том числе и правоохранительных, является информационно-просветительская деятельность об угрозе со стороны мошенников, действующих в сети Интернет. Достаточно активно ее осуществляет Центр мониторинга и реагирования на электронные атаки в кредитно-финансовой

сфере, являющийся структурой Департамента информационной безопасности Банка России.

Аферисты изобретают все новые и новые способы отъема денег у населения, однако, психологические методы воздействия остаются прежними. По статистике, именно чувство корысти и жажда наживы являются причиной преступлений в Интернете. При этом нельзя выделить какой-либо определенный метод решения сложившейся ситуации, так как все политические, экономические и социальные агенты должны действовать в совокупности и в полной мере обеспечивать финансовую безопасность субъектам в цифровой сфере.

Список литературы

1. Проблемы компьютерной преступности. – URL: https://vuzlit.ru/701281/problemy_latentnosti_kompyuternoy_prestupnosti

2. Министерство внутренних дел Российской Федерации. – URL: https://мвд.рф/reports/item/21551069/

3. Университет Банка России. – URL: https://university.cbr.ru/view_ doc.html?mode=szpp&doc_id=6656730423984475485

4. Уголовный кодекс Российской Федерации ст. № 159.6. «Мошенничество в сфере компьютерной информации». – URL: // http://www.consultant.ru/document/ cons_doc_LAW_10699/ 51c53d82b60ac8c009745bdea3838d507064c6d3/

References

1. Problems of computer crime [*Problemy komp'yuternoy prestupnosti*]. – URL: https://vuzlit.ru/701281/problemy_latentnosti_kompyuternoy_prestupnosti

2. Ministry of Internal Affairs of the Russian Federation [*Ministerstvo vnutrennikh del Rossiyskoy Federatsii*] // URL: https://мвд.рф/reports/item/21551069/

3. University of the Bank of Russia [*Universitet Banka Rossii*]. – URL: https://university.cbr.ru/view_doc.html?mode=szpp&doc_id=6656730423984475485

4. Criminal Code of the Russian Federation article No. 159.6. «Fraud in the field of computer information» [*Ugolovnyy kodeks Rossiyskoy Federatsii st. № 159.6. «Moshennichestvo v sfere komp'yuternoy informatsii»*]. – URL: //http://www.consultant.ru/ document/cons_doc_LAW_10699/51c53d82b60ac8c009745bdea3838d507064c6d3/