

**Ссылка для цитирования этой статьи:**

Глухов С.С. Вопросы противодействия преступности в сфере мошенничеств с использованием сотовой связи и средств массовой информации // Human Progress. 2024. Том 10, Вып. 6. С. 34. URL: [http://progress-human.com/images/2024/Tom10\\_6/Gluhov.pdf](http://progress-human.com/images/2024/Tom10_6/Gluhov.pdf) DOI 10.46320/2073-4506-2024-6a-31.

## **ВОПРОСЫ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПНОСТИ В СФЕРЕ МОШЕННИЧЕСТВ С ИСПОЛЬЗОВАНИЕМ СОТОВОЙ СВЯЗИ И СРЕДСТВ МАССОВОЙ ИНФОРМАЦИИ**

**Глухов Сергей Сергеевич**  
преподаватель кафедры профессиональных дисциплин  
факультет государственных и муниципальных служащих  
Самарский юридический институт ФСИН России  
г. Самара, Российская Федерация

**Аннотация.** Проблемы борьбы с преступностью в сфере мошенничеств с использованием сотовой связи и средств массовой информации имеет ключевое значение в современную цифровую эпоху. С быстрым развитием технологий, мобильные телефоны, социальные сети, средства массовой информации являются неотъемлемой частью нашей повседневной жизни, это делает нас уязвимыми для различных форм мошеннических действий, называемых, киберпреступлениями. В статье автор проанализировал историю развития сотовых мошенничеств в России, раскрыл ее разновидности, а также классифицировал их по уровню и степени общественной опасности. Отдельно в статье описываются текущее положение дел в сфере кибербезопасности, основные направления борьбы с киберпреступниками, сложности при статистическом учете преступлений и проблемы распределения компетенций между государственными и правоохранительными органами.

**Ключевые слова:** мошенничество с использованием сотовой связи, средства массовой информации, социальные сети, киберпреступность, противоправные действия, искусственный интеллект.

Данная категория преступлений представляет собой незаконные, виновные, противоправные действия, имеющие высокую степень общественной опасности, которые совершаются злоумышленниками путем использования сотовых или других устройств мобильной связи, а также средств массовой информации. Такой вид преступлений включается

в себя хищение денежных средств с банковских счетов, кражу личных данных, взлом, фишинг и другие различные формы мошенничества. Постоянный рост данной категории преступлений является значительной угрозой для отдельных категорий граждан, предприятий, а также общества в целом, приводя к финансовым потерям и краже интеллектуальной собственности.

Важность решения этой проблемы заключается в необходимости защитить население от возможных преступных посягательств, чтобы граждане не стали жертвами мошеннических схем. Поскольку злоумышленники продолжают использовать уязвимости в социальных сетях и устройствах мобильной связи, важно систематически разрабатывать эффективные стратегии и механизмы противодействия этой категории преступлений.

История мошенничества с использованием сотовой связи и средств массовой информации в России, как и во всем мире, развивалась постепенно, параллельно с развитием технологического прогресса и использования обществом различных видов гаджетов [1].

На ранних этапах, в 1980 - начало 1990 годов мошенничество с использованием информационных технологий выражалось в хищении информации, мошенничестве при использовании электронных счетов, а также в несанкционированном доступе к государственным базам данных. Обуславливалось это ограниченным доступом к компьютерам и Интернету, а также отсутствием соответствующей нормативно-правовой базой, регулирующей данные правоотношения.

Период рыночной экономики (1990-е года) характеризуется увеличением доступности сети интернет, а также распространением персональных данных, что в свою очередь создавало благоприятную среду для развития и модернизации преступлений в сфере использования информационных технологий. Появились новые виды таких преступлений как, финансовое мошенничество, кража личных данных, кибершпионаж, хакерские атаки.

В России к началу 2000-х годов, когда в стране наблюдался стремительный рост использования мобильных телефонов и различных интернет ресурсов. По мере того, как все больше людей начали использовать мобильные телефоны для связи и финансовых транзакций, злоумышленники начали использовать эту технологию для мошеннических действий, придумывая различные, изощренные методы хищения денежных средств.

К современным же тенденциям можно отнести стремительное развитие искусственного интеллекта, который может как способствовать борьбе с киберпреступностью, так и быть инструментом для совершения новых видов преступлений.

По мере того, как все больше людей начали использовать мобильные телефоны для связи и финансовых транзакций, злоумышленники начали использовать эту технологию для

мошеннических действий, придумывая различные, изощренные методы хищения денежных средств.

Одним из наиболее распространенных видов мошенничества с использованием сотовой связи в России является "фишинг". Фишинг (с английского phishing от fishing "рыбная ловля, выуживание" - это вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей, таким как логины и пароли. Как правило, данный вид преступлений достигается путём проведения массовых рассылок электронных писем от имени популярных брендов, а также личных сообщений внутри различных сервисов, например, от имени банков или внутри социальных сетей. В письме часто содержится прямая ссылка на сайт, внешне неотличимый от настоящего, либо на сайт с редиректом. После того, как пользователь попадает на поддельную страницу, мошенники пытаются различными психологическими приёмами побудить пользователя ввести на поддельной странице свои логин и пароль, которые он использует для доступа к определённому сайту, что позволяет мошенникам получить доступ к аккаунтам и банковским счетам<sup>1</sup>.

Другим распространенным видом сотовых мошенничеств является "спуфинг". Спуфинг (с английского Spoofing- подделка) это вид киберпреступлений, при котором злоумышленники используют различные технологии, при помощи которых осуществляют подмену входящего номера, создавая впечатление, что звонок исходит от авторитетной организации, такой как банк, государственное учреждение или знакомый человек. Такой способ направлен на манипуляцию эмоциями потенциальной жертвы, с целью получить доступ к ее личной информации или деньгам. Например, злоумышленники часто используют сценарий "родственника в беде", представляясь близкими родственниками жертвы, находящимися в затруднительном положении. Такой способ направлен на манипуляцию эмоциями потенциальной жертвы, с целью получить доступ к ее личной информации или денежным средствам [2].

В целом, мошенничества с использованием сотовой связи и средств массовой информацией стали серьезной проблемой в России. Представленные официальные данные МВД России за первый период 2024 года показывают, что число преступлений данной категории выросло на 39,3% по сравнению с аналогичным периодом прошлого года. В период с января по июль 2024 года зарегистрировано более 210,8 тысяч различных мошенничеств. В

---

<sup>1</sup> Национальные правовые режимы России и Франции в сфере цифровой безопасности: компаративный анализ (Кожевина О. В.) ("Право и цифровая экономика", 2020, N 2). Доступ из СПС «КонсультантПлюс».

числе данных хищений значительна доля (79,1%) мошенничеств, совершенных дистанционно, с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации (166,8 тысяч). Темп их роста, относительно первого полугодия прошлого года увеличился на 40,5%. Ущерб от таких преступлений, совершенных в 2024 году, уже составляет 99 млрд рублей. Сумма ущерба от таких случаев за весь 2023 год составила 156 млрд рублей.

Проанализировав представленные сведения, можно сделать вывод, что вопрос кибербезопасности имеет острое социальное значение в современном обществе, так как злоумышленники не стоят на месте и постоянно совершенствуют свои преступные схемы, используя все более изощренные техники обмана.

Для того, чтобы сменить тенденцию роста в сторону снижения указанной категории преступлений, необходимо принятие соответствующих комплексных мер, таких как внесение изменений в нормативно-правовые акты регулирующие правоотношения в данной области, например, в ФЗ № 152 от 27.07.2006 «О персональных данных», необходимо ужесточить меры по сбору и хранению персональных данных<sup>2</sup>.

Закон № 152-ФЗ устанавливает общие принципы обработки персональных данных, права субъектов персональных данных, обязанности операторов, контроль за соблюдением законодательства. Указанный Федеральный закон соответствует международным стандартам, содержит ряд положения отражающие принципы и требования международных положений по защите персональных данных, например, принципы обработки данных по General Data Protection Regulation (GDPR).

Контроль за соблюдением правовых основ закона № 152-ФЗ возложена на Роскомнадзор, но в реальности ему не всегда удается эффективно реагировать на огромное количество различных нарушений. Связанно это с отсутствием единого реестра операторов, что усложняет контроль за их деятельностью.

В свою очередь закон о защите персональных данных недостаточно структурирован, что приводит к неоднозначному толкованию его правовых норм. Например, не достаточно конкретно определен порядок для получения согласия субъекта на обработку персональных данных, также нечетко определены понятия "анонимизация", "деперсонализация" [3].

---

<sup>2</sup> Закон от 27.07.2006 N 152-ФЗ (ред. от 08.08.2024) "О персональных данных" Доступ из СПС «КонсультантПлюс».

Также закон № 152-ФЗ не предусматривает алгоритм действий, препятствующий незаконной передаче персональных данных за границу, особенно в отношении иностранных компаний. Штрафные санкции в данной сфере не содержат превентивный характер и не сдерживают недобросовестных операторов.

Правоохранительные органы должны выступать главным субъектом профилактики, пресечения и предупреждения данной категории преступлений. На постоянной основе должна проводиться работа с населением, целью которой будет просвещение граждан о методах и способах защиты от мошенничеств с использованием сотовой связи, повышения их юридической грамотности.

Важно помнить, что основная защита от любых видов сотовых мошенничеств лежит на плечах каждого пользователя мобильных устройств. Необходимо проявлять повышенную бдительность и не доверять незнакомым звонкам, не раскрывать личную информацию и использовать современные средства защиты. Также не стоит принимать поспешных решений, решений под давлением, проявлять внимание к деталям, задавать большое количество вопросов. Злоумышленники не стоят на месте и постоянно придумывают новые, более изощренные способы для осуществления своих преступных замыслов, поэтому только совместные усилия могут помочь снизить киберпреступность в России и обеспечить финансовую безопасность граждан.

### Список литературы

1. Петров И. Мошенники ушли в Сеть. Резко выросло число преступлений, совершаемых с помощью IT-технологий / И. Петров // Российская газета. Федеральный выпуск. 2020. 28 января.
2. Трунцевский Ю.В. Криминальные угрозы электронной коммерции: международные и национальные аспекты / Ю.В. Трунцевский, К.В. Кецко // Международное публичное и частное право. 2020. № 6. С. 18 - 22.
3. Трунцевский Ю.В. Цифровая интеграция - путь в будущее / Ю.В. Трунцевский, А.А. Ефремов // Международное публичное и частное право. 2018. № 1. С. 6 - 12.

# ISSUES OF COMBATING CRIME IN THE FIELD OF FRAUD USING CELLULAR COMMUNICATIONS AND MASS MEDIA

**Glukhov Sergey Sergeevich**

Teacher of the Department of Professional Disciplines  
Faculty of State and Municipal Employees  
Samara Law Institute of the Federal Penitentiary Service of Russia  
Samara, Russian Federation

**Abstract** the problems of combating crime in the field of fraud using cellular communications and mass media are of key importance in the modern digital era. With the rapid development of technology, mobile phones, social networks, and the media are an integral part of our daily lives, making us vulnerable to various forms of fraudulent activities called cybercrimes. In the article, the author analyzed the history of the development of cellular fraud in Russia, revealed its varieties, and classified them according to the level and degree of public danger. Separately, the article describes the current state of affairs in the field of cybersecurity, the main directions of combating cybercriminals, the difficulties in statistical accounting of crimes and the problems of the distribution of competencies between state and law enforcement agencies.

**Keywords:** fraud using cellular communications, mass media, social networks, cybercrime, illegal actions, artificial intelligence.

## References

1. Petrov I. The scammers went online. The number of crimes committed with the help of IT technologies has increased dramatically / I. Petrov // Rossiyskaya Gazeta. Federal issue. 2020. January 28.
2. Truntsevsky Yu.V. Criminal threats to e-commerce: international and national aspects / Yu.V. Truntsevsky, K.V. Ketsko // International public and private law. 2020. № 6. P. 18-22.
3. Truntsevsky Yu.V. Digital integration - the way to the future / Yu.V. Truntsevsky, A.A. Efremov // International public and private law. 2018. № 1. P. 6-12.