

МАЙСТРЕНКО Григорий Александрович,

кандидат юридических наук,

старший научный сотрудник ФКУ НИИ ФСИН России,

ORCID: 0000-0001-5668-615X,

e-mail: g.maystrenko@yandex.ru

НОВЫЕ ТЕНДЕНЦИИ В БОРЬБЕ С КИБЕРПРЕСТУПНОСТЬЮ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Аннотация. Настоящая статья посвящена выявлению новых тенденций в борьбе с киберпреступностью в Российской Федерации в последние годы. Автор сосредотачивает внимание на причинах роста преступной активности в цифровой среде, связи динамики противоправных преступных деяний с возникновением и расширением нового поля для их совершения – онлайн-пространством.

В работе сделан важный вывод о том, что противодействие преступной активности, реализуемой по основным коммуникационным каналам – сети Интернет, социальным сетям, а также телефонной связи, требует самостоятельных мер борьбы, а также массового информирования российских граждан, внедрения антимошеннических цифровых программ.

Ключевые слова: киберпреступность, цифровизация, цифровая среда, социальные сети, интернет, мошенничество.

MAISTRENKO Grigoriy Aleksandrovich,

senior researcher of the PKU RESEARCH INSTITUTE

of the Federal Penal Correction Service, PhD

NEW TRENDS IN THE FIGHT AGAINST CYBERCRIME IN THE RUSSIAN FEDERATION

Annotation. This article identifies new trends in the fight against cybercrime in the Russian Federation in recent years. The author focuses on the causes of the growth of criminal activity in the digital environment and the connection between the dynamics of illegal crimes and the emergence and expansion of a new medium for their commission – the online space.

The paper draws an important conclusion: countering criminal activity conducted through primary communication channels – the internet, social media, and telephone – requires independent countermeasures, as well as mass awareness raising for Russian citizens and the implementation of anti-fraud digital programs.

Key words: cybercrime, digitalization, digital environment, social media, internet, fraud.

В настоящее время неуклонно возрастает количество правонарушений, совершенных в цифровом пространстве, либо с использованием цифровых технологий в России и на международном поле. Ситуацию распространения киберпреступности не стоит недооценивать. Согласно открытой статистике последних лет, представленной МВД России, количество преступлений в информационном пространстве имеет стабильную тенденцию к росту[6.с. 250]. Появление нового вида преступлений - престу-

плений в области компьютерной информации - обусловило включение в 1996 г. в УК РФ соответствующей главы 28[7]. Отечественный законодатель принял решение включить указанную главу в УК РФ в силу того, что соответствующие посягательства, появившись и распространившись в зарубежных странах, стали совершаться и в Российской Федерации[8]. На основании данных по состоянию киберпреступностью в мире, 25-26 октября в Ханое уполномоченные представители 71 государства подписали Конвенцию ООН про-

тив киберпреступности (Конвенция). В соответствии с распоряжением Президента Российской Федерации В.В.Путина от 23 октября 2025 года № 409-рп Генеральный прокурор Российской Федерации А.В.Гуцан подписал Конвенцию, а также огласил приветственное послание В.В.Путина участникам и гостям церемонии. В послании отмечено, что, несмотря на непростую международную обстановку, дипломаты и представители правоохранительных органов государств-членов ООН смогли объединить усилия, чтобы согласовать Конвенцию[5].

Проникновение достижений цифровизации в различные сферы жизни современного российского общества отнюдь не всегда играет положительную роль, но также оказывает отрицательное воздействие в силу того, что цифровая среда стала новым пространством для совершения противоправных преступных деяний. В свою очередь, непрерывное совершенствование цифровых технологий обуславливает возникновение все новых видов и форм преступлений, совершаемых в онлайн-среде. В этой связи, справедливым представляется вывод Главного информационно-аналитического центра МВД России (ГИАЦ МВД РФ), сделанный на базе анализа статистических материалов, в соответствии с которым современная реальность представляет собой настоящий скачок в области развития информационных отношений, телекоммуникационных систем, компьютерных технологий, а также социальных сетей. Он характеризуется возникновением новых средств конструирования, хранения, обработки, а также трансляции сведений в цифровом формате, расширением границ киберпространства и, наконец, тотальным охватом социума процессами компьютеризации [4].

Несмотря на то, что в своем выступлении от 4 марта 2026 г. Президент Российской Федерации – Владимир Владимирович Путин заявил, что количество киберпреступлений, совершенных, в том числе, против пенсионеров – в последнее время сократилось, что, в свою очередь, является результатом системных мер, реализуемых МВД России, а также иными правоохранительными органами и специальными службами, борьба с киберпреступниками, по мнению главы российского государства, требует серьезного внимания [2]. В первую очередь, это объясняется тем, что в РФ, как и в других странах мира, существуют категории граждан, в большей степени, по сравнению с иными, подверженные действиям киберпреступников. Граждане старшего возраста являются наиболее социально уязвимой группой относительно атак правонарушителей, действующих в цифровом пространстве. В первую очередь, это объясняется тем, что пенсионеры в силу

возраста не обладают достаточным уровнем знаний в области современных технологий, с трудом обучаются новому, тем более – в цифровой среде. Как следствие, сложной задачей для них выступает полноценная интеграция в современную реальность, перенасыщенную технологиями, действующими на базе цифровых платформ. Кроме того, большинство лиц пенсионного возраста являются доверчивыми, в силу чего значительно чаще попадают на уловки мошенников [3].

Последние изменения российского законодательства также отражают исследуемую проблему в обществе, необходимость усовершенствования механизмов противодействия киберпреступности[1].

Необходимо отметить, что системность действий МВД и специальных служб в борьбе с киберпреступностью проявляется, в том числе, в том, что меры борьбы против преступности имеют не только комплексный, но также адресный характер. В частности, к действиям общего характера следует отнести массовое информирование населения, а также внедрение антимошеннических сервисов, препятствующих тому, чтобы граждане российского государства страдали от действий цифровых преступников. Между тем, несмотря на широкое применение вышеперечисленных мер население продолжает попадаться на уловки мошенников. Наиболее распространенные каналы совершения преступлений в цифровом пространстве представлены на *рисунке 1*.

Таким образом, на основе рисунка 1 можно заключить, что основными каналами совершения противоправных преступных деяний в цифровой среде являются телефонная связь, пространство сети Интернет, а также социальных сетей. Иными словами, расширение каналов коммуникации в последнее десятилетие обусловило возникновение новых видов противоправных преступных деяний. В свою очередь, киберпреступники избрывают для своих жертв хитроумные ловушки, ориентируясь на наиболее часто используемые последними каналы коммуникации. Логично предположить, что граждане преклонного возраста чаще подвергаются атаке преступников через телефонные звонки, в то время как население молодого и среднего возраста может пострадать от мошеннических действий в сети Интернет, а также в социальных сетях. Однако на практике не исключено совмещение указанных каналов в совершении правонарушений в цифровой среде. В наиболее общем виде схему противодействия киберпреступности по каждому из обозначенных выше направлений можно представить в виде *рисунка 2*.

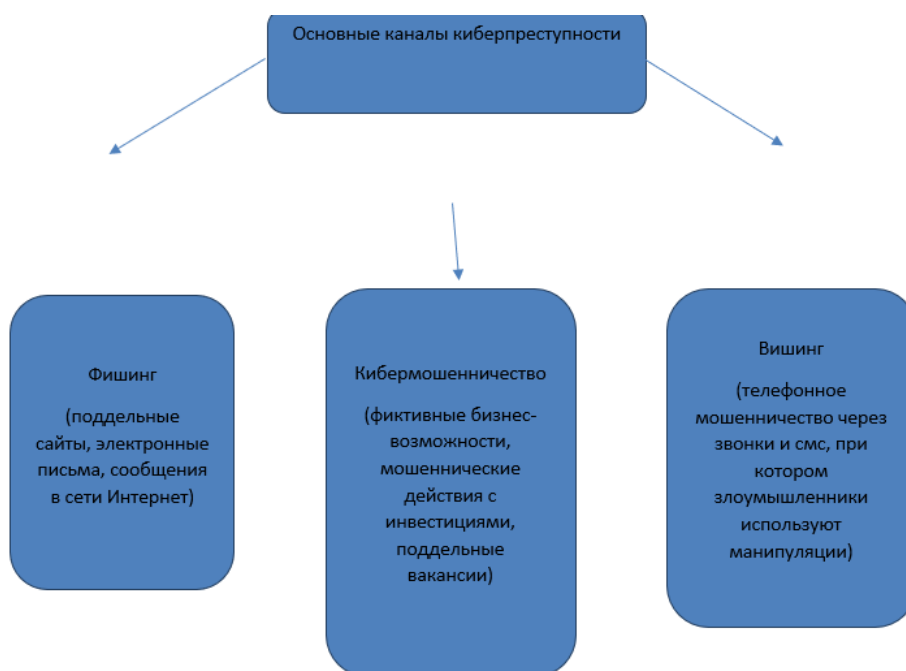


Рис.1.Основные каналы совершения преступлений в цифровом пространстве



Рис. 2. Способы противодействия отдельным видам киберпреступности

Таким образом, мы видим, что противодействие наиболее распространенным видам правонарушений, реализуемым в цифровой среде, состоит, прежде всего в защите личных данных, получение доступа к которым является главной целью киберпреступников. Это определяется тем, что информация личного характера открывает доступ к счетам, аккумулирующим денежные средства жертвы (банковской карте, банковскому счету), а также к конфиденциальным сведениям, которые могут быть использованы преступниками в целях манипуляции и шантажа.

Подводя итоги рассмотрению вопроса о новых тенденциях в борьбе с киберпреступностью в Российской Федерации следует отметить, что они определяются непрерывностью возникновения все новых угроз в цифровом пространстве, их совершенствованием преступниками. К тенденциям последних лет в борьбе с киберпреступностью, прежде всего, относится тенденция на противодействие отдельным видам правонарушений, совершаемым по определенным каналам реализации преступной активности: в сети Интернет, социальных сетях, по телефону. Эффективная борьба с киберпреступностью зависит от грамотной разработки мер, направленных на борьбу с мошенничеством в киберпространстве.

Список литературы:

[1] Федеральный закон от 01.04.2025 N 41-ФЗ (ред. от 31.07.2025) «О создании государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации» // КонсультантПлюс: справочно-правовая система [Официальный сайт]. URL: <https://www.consultant.ru/> (дата обращения: 12.03.2026).

[2] Путин: Общее число киберпреступлений в РФ сократилось в 2025 году // RG.RU. 04.03.2026. URL: https://rg.ru/2026/03/04/putin-obshchee-chislo-kiberprestuplenij-v-rf-sokratilos-v-2025-godu.html?utm_referrer=https%3A%2F%2Fyandex.ru%2F (дата обращения: 12.03.2026).

[3] Семеняченко А.А. Кибермошенничество и кибербезопасность: как защитить пенсионеров и уязвимые слои общества / А.А. Семеняченко, Д.А. Семеняченко, Н.Ж. Имамова // Юный ученый. 2025. № 11 (96). – С. 60-63.

[4] Состояние преступности в России за январь – декабрь 2021 года / МВД ФКУ «Глав-

ный информационно-аналитический центр». – М., 66 с.

[5] Распоряжение Президента Российской Федерации В.В.Путина от 23 октября 2025 года № 409-рп.

[6] Никиташенко, В. В. Понятие и признаки киберпреступности / В. В. Никиташенко. — Текст: непосредственный // Молодой ученый. — 2021. — № 14 (356). — С. 250-252. — URL: <https://moluch.ru/archive/356/79639>.

[7] Уголовный кодекс Российской Федерации» от 13.06.1996 № 63-ФЗ (посл. ред.) [Электронный ресурс] // КонсультантПлюс.—URL: <https://www.consultant.ru/> (дата обращения: 12.03.2026).

[8] Марк Борисиков. Понятие и отличительные особенности киберпреступлений.

References:

[1] Federal Law of 01.04.2025 N 41-FZ (ed. 31.07.2025) “ On the creation of a state information system for countering offenses committed using information and communication technologies and on amending certain legislative acts of the Russian Federation “//ConsultantPlus: reference and legal system [Official website]. URL: <https://www.consultant.ru/> (access date: 12.03.2026).

[2] Putin: The total number of cybercrimes in the Russian Federation decreased in 2025//RG.RU. 04.03.2026. URL: https://rg.ru/2026/03/04/putin-obshchee-chislo-kiberprestuplenij-v-rf-sokratilos-v-2025-godu.html?utm_referrer=https%3A%2F%2Fyandex.ru%2F (accessed on: 12.03.2026).

[3] Semenyachenko A.A. Cyber fraud and cybersecurity: how to protect pensioners and vulnerable segments of society/A.A. Semenyachenko, D.A. Semenyachenko, N.Z. Imamova//Young scientist. 2025. № 11 (96). - S. 60-63.

[4] The state of crime in Russia in January-December 2021/Ministry of Internal Affairs of the PKU “Main Information and Analytical Center.” - M., 66 p.

[5] Order of the President of the Russian Federation V.V. Putin dated October 23, 2025 No. 409-rp.

[6] Nikitashenko, V.V. The concept and signs of cybercrime/V.V. Nikitashenko. - Text: direct//Young scientist. — 2021. — № 14 (356). - S. 250-252. — URL: <https://moluch.ru/archive/356/79639>.

[7] Criminal Code of the Russian Federation” dated 13.06.1996 No. 63-FZ (last ed.) [Electronic resource]//ConsultantPlus.—URL: <https://www.consultant.ru/> (date of contact: 12.03.2026).

[8] Mark Borisikov. The concept and distinctive features of cybercrimes.

