международном законе[1]. История фантастических проектов о космосе и космического права показывает, что процессы воображения и фиксации воображаемого в культуре со временем могут стать законом, а впоследствии и политикой[2]. В этом случае можно утверждать, что воображение порождает тревогу и неотложные потребности, которые ученые-юристы и технологи направляют в сторону права.

В заключение отметим, что будущее в настоящем. Социотехнологические фантазии – это приглашение законодателей идти в ногу со временем, чтобы изменения в законодательстве, принятые сейчас, обеспечили преимущества в будущем. Чтобы эти изменения были приняты, необходимо переформатировать правовое сознание в сторону принятия культурных инициатив и понимания правовых изменений как необходимости. Однако если воспринимать ажиотаж по поводу новых технологий как негатив для сознания, то достижение нового правосознания, основанного на разумном, рациональном праве, становится проблематичным. Необходимо использовать фантастические проекты как призыв к размышлению не только в форсайт-технологиях, но и правотворчестве, направляя усилия на создание нормативных режимов, которые могут гарантировать будущее, предотвращать мрачные страхи и обеспечивать взаимодействие права и технологии в настоящем и будущем.

Передерий В.А.,

кандидат социологических наук, доцент
Краснодарский университет МВД России (г. Краснодар)

Вельмисеева А.Н.,

Краснодарский университет МВД России (г. Краснодар)

Киберпреступность и кибермошенничество как угроза информационной безопасности России

За последние годы количество пользователей в социальных сетях резко возросло, они стали неотъемлемой частью жизни большинства россиян. Цифровые платформы предоставляют уникальную возмож-

[1] Договор о принципах деятельности государств по исследованию и использованию космического пространства, включая Луну и другие небесные тела (Договор о космосе) : принят резолюцией 2222 (XXI) Генеральной Ассамблеи от 19.12.1966, подписан в Лондоне, Москве и Вашингтоне 27.01.1967, вступил в силу 10.10.1967. Договор бессрочный. URL: https://www.un.org/ru/documents/decl_conv/con-ventions/outer_space_governing.shtml (дата обращения: 01.09.2025).

[2] Вылегжанин А.Н., Юзбашян М.Р. Указ. соч.

ность для общения, обмена информацией из любого уголка мира, что еще в конце прошлого столетия казалось невозможным. Однако, несмотря на положительные аспекты, с развитием технологий и увеличением количества пользователей в сети Интернет возросло и количество преступлений в сфере компьютерной информации, отражающее трансграничный характер, что затрудняет их расследование и раскрываемость. Параллельно с этим наблюдается устойчивый рост числа жертв мошенничества в социальных сетях. Современные технологии, включая искусственный интеллект и нейросети, способствуют развитию новых методов и способов мошенничества, делая преступников неуязвимыми в условиях цифровой среды.

Для более глубокого понимания текущего состояния преступности в сфере информационно-телекоммуникационных технологий было проведено социологическое исследование с помощью контент-анализа. По официальным данным МВД России, начиная с января 2025 года было зарегистрировано 247202 преступления, из которых раскрыто всего лишь 69304, что составляет 28,03 % от общего числа преступлений в сфере компьютерной информации. Самыми распространенными из них являются кражи и мошенничества. Больше всего зарегистрировано преступлений в следующих регионах Российской Федерации: Чеченская Республика, Республика Саха (Якутия), Камчатский край, Ханты-Мансийский АО – Югра, Республика Дагестан, Забайкальский край, Магаданская область, Ставропольский край, Рязанская область и Иркутская область. Субъектами с наименьшими темпами прироста зарегистрированных преступлений являются Чукотский АО, Ненецкий АО, Новгородская область, Курская область, Тверская область, Архангельская область, Псковская область, Республика Мордовия, Мурманская область, Республика Татарстан. При этом именно в регионах, где больше всего зарегистрировано преступлений, раскрываемость значительно выше[1].

В 2024 году, по данным опроса, проведенного ЦБ РФ, жертвами мошенников чаще всего становились женщины в возрасте 25–44 лет со средним уровнем дохода и средним образованием, живущие в городах. Они переходили по подозрительным ссылкам, сообщали личные данные и добровольно переводили деньги. Основные методы, которые использовали злоумышленники – телефонное и СМС-мошенничество, доступ к аккаунтам на Госуслугах. Потери составляли до 20 тыс. рублей, однако возросло количество крупных переводов (100–500 тыс. рублей). Более

[1] Краткая характеристика состояния преступности в Российской Федерации за январь – апрель 2025 г. // Официальный сайт Министерства внутренних дел Российской Федерации. URL: https://xn--b1aew.xn--p1ai/reports/item/65027102 (дата обращения: 16.06.2025).

70 % потеряли личные сбережения, 15 % – кредитные средства. Большинство (42,8 %) обращались в банк, 30 % – в полицию[1].

Злоумышленники используют различные методы и виды мошенничества в интернете, нацеливаясь не только на взрослых, но и на более уязвимую группу – несовершеннолетних. Частыми способами становятся рассылка фишинговых сообщений и ссылок, которые выглядят как официальные уведомления от знакомых, банков, государственных учреждений и других организаций, однако преследуют одну цель – выманить личные данные и конфиденциальную информацию. Кроме того, мошенники могут размещать в социальных сетях вредоносные ссылки, прикреплять файлы, содержащие вирусы или шпионские ПО. За последнее время в сети наблюдается следующая тенденция: пользователь публикует пост на своей странице в социальной сети. После публикации под этим постом появляются хейтерские комментарии, содержащие элементы социальной инженерии, например: «Все-таки хорошо, что мы перестали общаться… Сильно жизнь тебя потрепала…», что побуждает любопытство со стороны пользователя. Эти комментарии создают иллюзию личного интереса и стимулируют пользователя к переходу на страницу комментатора. После перехода по этой ссылке преступники взламывают аккаунт и получают доступ к конфиденциальной информации. Данная схема является классическим примером социальной инженерии, направленной на компрометацию личных данных пользователя. С начала 2024 года активно применяются технологии спуфинга, которые с развитием технологий на сегодняшний момент эволюционировали настолько, что мошенники могут в режиме реального времени генерировать видеосообщения, изменять голос, который невозможно отличить от голоса родственника, коллеги, знакомого в мессенджерах.

Анализ распространенных способов совершения преступлений в сфере компьютерной информации с использованием социальных сетей показал, что киберпреступники чаще применяют их для своих махинаций. Это связано с тем, что за последние годы данная платформа приобрела большую популярность. На сегодняшний день в ней насчитывается более 1 миллиарда активных пользователей. С учетом существующей тенденции мы выделили ряд проблем, способствующих распространению мошеннических схем в социальных сетях.

Во-первых, это связано с участившимися кражами аккаунтов. Так, на первый квартал 2025 года насчитывается около 887 тысяч краж

[1] Портрет пострадавшего от кибермошенников в 2024 году // Официальный сайт Банка России. URL: https://cbr.ru/press/event/?id=23367 (дата обращения: 16.06.2025).

профилей. Во-вторых, преступники помимо перечисленных выше способов, таких как фишинг, спуфинг, социальная инженерия, используют подделку интерфейса данного мессенджера, имитируют службу поддержки, стремясь похитить данные жертвы. Они могут заявить, что возникли проблемы с аккаунтом, и потребовать пароль или другие сведения для устранения неисправности. Люди, считая, что с ними связалась техническая поддержка, сами передают всю необходимую для мошенников информацию. В-третьих, зарубежные мессенджеры не осуществляют мониторинг за личными переписками и контентом, который размещают пользователи в своих закрытых каналах, соответственно данное обстоятельство способствует распространению запрещенных материалов среди аудитории, в числе которой могут быть дети и подростки.

Стоит также отметить, что государство активно занимается разработкой программ, которые могли бы обезопасить граждан от кибермошенничества. Так, например, Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации в июне 2025 года планируется разработка мобильного приложения, которое оповещало бы население о предстоящем мошенническом действии, а также имело бы «тревожную кнопку» для защиты от злоумышленников. «Две основные, наверное, задачи – это онлайн-информирование гражданина о том, что прямо сейчас в отношении него может осуществляться мошенническое действие. И второе – это «тревожная кнопка», которую гражданин может нажать в случае, если он считает, что у него происходят какие-то необычные события. По любому случаю мошенничества он может сюда обратиться», – приводит слова замминистра РИА Новости[1].

Правительством Российской Федерации также разрабатывается комплекс мер по борьбе с кибермошенничеством. Так, с 2022 года в России начала работать платформа «Антифишинг», которая осуществляет поиск и анализ сайтов, потенциально используемых мошенниками, блокирует фишинговые сайты и оповещает жителей о возможных угрозах. Помимо этого, поступила инициатива о создании цифровой платформы, которая должна объединить всех участников процесса с целью противодействия киберпреступности. Государственным органам будет предоставлена возможность оперативно осуществлять мониторинг и производить анализ киберпреступлений, что позволит более эффективно блокировать мошенническую деятельность. Банковские организации и учреждения смогут незамедлительно приостанавливать подозрительные

[1] Минцифры разработает приложение для защиты от кибермошенничества // Официальный сайт Парламентской газеты. URL: https://www.pnp.ru/social/v-rossii-poyavitsya-prilozhenie-dlya-zashhity-ot-kibermoshennichestva.html (дата обращения: 16.06.2025)

переводы и транзакции. Операторы связи будут оснащены инструментами для выявления подозрительных телефонных звонков и оперативного блокирования SIM-карт, которые используют преступники. Еще одной постепенно вводимой мерой является запрет на использование иностранных мессенджеров в служебных целях и на их применение в коммуникации между сотрудниками банковских учреждений, государственных органов и операторов связи. Данное предложение основывается на необходимости обеспечения высокого уровня информационной безопасности и защиты конфиденциальных данных, так как иностранные мессенджеры, несмотря на свое удобство и популярность, не могут гарантировать достаточный уровень защиты информации[1].

С целью минимизации рисков, связанных с мошеннической деятельностью в социальных сетях, пользователям предлагается ряд рекомендаций, основанных на глубоком анализе современных угроз информационной безопасности и методов их нейтрализации:

1) развивать навыки критического мышления и способность распознавать признаки мошеннических схем (подвергать сомнению любую информацию, полученную через социальные сети);

2) внимательно относиться к излишне привлекательным предложениям в социальных сетях (высокий заработок, гарантированные выигрыши);

3) изучать информацию о каждом контакте, включая «аватарки», описание профиля и сообщения с проверкой информации о контакте в других источниках;

4) использовать надежные методы оплаты в сетях. Не отправлять денежные средства через непроверенные источники и не предоставлять данные банковских карт и другую конфиденциальную информацию по телефону, в электронных письмах или в сообщениях;

5) осуществлять тщательную верификацию защищенного соединения (https://) и внимательно изучать URL-адрес сайта, используя надежные пароли и двухфакторную аутентификацию.

Результаты проведенного исследования показывают, что уровень раскрываемости преступлений в сфере информационно-телекоммуникационных технологий остается крайне низким, что свидетельствует о необходимости внедрения и разработки технологий, способствующих эффективному мониторингу и предотвращению подобных преступлений. Необходимо повышать цифровую грамотность граждан, вести

[1] Как защитят граждан от кибермошенников: новые меры борьбы // Официальный сайт Парламентской газеты. URL: https://www.pnp.ru/social/kak-zashhityat-grazhdan-ot-kibermoshennikov-novye-mery-borby.html (дата обращения: 16.06.2025)

просвещенческую работу, информируя население о возможных угрозах для своевременного распознания, и защищать персональных данные в цифровом пространстве.

Тепляшин П.В.,

доктор юридических наук, профессор
Сибирский юридический институт МВД России (г. Красноярск)

Антикриминальное право как самостоятельная отрасль российского права: гипотетическая перспектива и обуславливающие факторы

Современная траектория развития дисциплин криминального цикла указывает на формирование новых юридических образований, ориентированных на всемерное обеспечение антикриминальной (от лат. *criminalis* – преступный) безопасности. Нормативные скрепы такой траектории стали приобретать более-менее отчетливый вид в связи с принятием Федерального закона от 23 июня 2016 года № 182-ФЗ «Об основах системы профилактики правонарушений в Российской Федерации» (далее – Федеральный закон о профилактике), который выступил генерирующим основанием построения системы правового воздействия на общественные отношения, возникающие и существующие по поводу профилактики преступности. В этой связи В.А. Зикеев верно отмечает, что формирование в России системы законодательства связано с возникновением правовых интегративных явлений, протекающих параллельно с процессом дифференциации и автономизации нормативного регулирования. Не является исключением в этом отношении и законодательство о противодействии преступности[1].

Система такого воздействия потребовала дальнейшего формирования новых «фактурных» юридических образований, которые можно идентифицировать через правовые отраслевые механизмы. Так, можно говорить о фактическом зарождении, например пробационного права, что обусловлено принятием Федерального закона от 6 февраля 2023 го-да № 10-ФЗ «О пробации в Российской Федерации», который в ч. 1 ст. 4 одной из целей пробации закрепляет предупреждение совершения осужденными новых преступлений.

В силу отмеченной методологической преамбулы можно утверждать, что отечественная правовая система находится на заре появления

[1] Зикеев В.А. О криминологической отрасли права // Криминология: вчера, сегодня, завтра. 2019. № 4. С. 74.