***Соловьева Людмила Юрьевна***
магистрант
УВО «Университет управления «ТИСБИ»
г. Казань, Республика Татарстан

# РОЛЬ СРЕДСТВ МАССОВОЙ ИНФОРМАЦИИ В СИСТЕМЕ НЕФОРМАЛЬНОГО СОЦИАЛЬНОГО КОНТРОЛЯ НАД КИБЕРПРЕСТУПНОСТЬЮ

***Аннотация:*** *в статье анализируется роль средств массовой информации в системе неформального социального контроля над киберпреступностью. Рассматриваются теоретические аспекты неформального социального контроля, его функции и механизмы. На основе анализа актуальных законодательных инициатив, материалов круглого стола «Алгоритмы самозащиты: роль СМИ в схватке с кибермошенничеством», а также практического опыта взаимодействия правоохранительных органов и журналистов обосновывается ключевая роль СМИ в формировании у граждан алгоритмов самозащиты и правового просвещения. Предлагаются конкретные направления повышения эффективности информационного воздействия СМИ в сфере противодействия киберпреступности.*

***Ключевые слова:*** *киберпреступность, неформальный социальный контроль, СМИ, правовое просвещение, цифровая грамотность, алгоритмы самозащиты, профилактика преступлений.*

В условиях стремительной цифровизации всех сфер жизнедеятельности общества проблема киберпреступности перестала быть узкоспециализированным вызовом для правоохранительных органов и трансформировалась в один из ключевых факторов, дестабилизирующих национальную безопасность и устойчивость правопорядка. Масштабы данного феномена приобретают характер эпидемии: по итогам 2025 года доля преступлений, совершенных с использованием информационно-телекоммуникационных технологий, достигла 40% от общего числа зарегистрированных деяний, что в абсолютных цифрах выражается в

675 тысячах возбужденных уголовных дел. Эти статистические показатели красноречиво свидетельствуют не только о росте технической оснащенности криминальных элементов, но и о глубинном системном сдвиге в структуре общественных отношений, где виртуальное пространство становится основной ареной противоправных действий.

Парадоксальность текущей ситуации усугубляется разнонаправленными векторами развития: с одной стороны, мы наблюдаем неуклонное снижение общего уровня цифровой грамотности населения, особенно среди возрастных и социально уязвимых групп, а с другой – стремительное повышение изощренности преступных схем, включающих элементы социальной инженерии, психологического манипулирования и использования алгоритмов искусственного интеллекта. В этих условиях классические правовые (формальные) инструменты противодействия, базирующиеся на системе запретов, санкций и процессуальных норм, демонстрируют свою ограниченную эффективность. Как справедливо отмечается в современной криминологической литературе, девиантные отношения в цифровой среде глубоко укоренены в системе неформальных практик, повседневных коммуникаций и стихийно складывающихся социальных норм, что делает их малодоступными для прямого правового воздействия. Именно поэтому на передний план выходит необходимость развития неформальных механизмов социального контроля, способных работать на упреждение, формируя у граждан внутренние барьеры и установки, препятствующие переходу девиантных отношений в институционализированную преступную систему.

В данном контексте средства массовой информации (СМИ) приобретают статус стратегического актора, занимая особое, институционально значимое место в механизме неформального контроля. Функциональный потенциал СМИ далеко выходит за рамки простого информирования: они выступают в роли трансляторов социальных норм, агрегаторов общезначимых ценностей, каналов правового просвещения и инструментов формирования коллективной резистентности к киберугрозам. Как образно выразился сенатор Сергей Перминов, «если до конкретного человека информация не будет доведена в доступной форме, то все,

что мы будем делать, будет «обнуляться». Эта метафора точно схватывает суть проблемы: любые усилия государства, законодательные инициативы и полицейские операции останутся невостребованными, если они не будут подкреплены массированной, адресной и понятной информационно-разъяснительной работой на всех уровнях социальной стратификации.

Цель настоящей статьи состоит в комплексном анализе роли СМИ в системе неформального социального контроля над киберпреступностью. В рамках достижения этой цели предполагается решить следующие задачи: во-первых, теоретически обосновать разграничение формальных и неформальных механизмов контроля применительно к цифровой среде; во-вторых, выявить специфические функции медиа в профилактике киберпреступлений; в-третьих, на основе анализа актуальных законодательных инициатив и практических кейсов предложить пути повышения эффективности информационного воздействия, а также сформулировать этические принципы освещения данной проблематики.

В современной социолого-правовой науке категория «социальный контроль» традиционно рассматривается в дихотомии формального (институционального) и неформального (неинституционального) измерения. Формальный контроль олицетворяет собой систему государственных институтов (суд, прокуратура, полиция, органы исполнительной власти), действующих на основе жестко кодифицированных правовых норм и обладающих легитимным правом применения принудительных санкций. Его сила – в императивности, универсальности и формальной определенности, однако его слабость обнаруживается именно в сфере киберпреступности, где юрисдикционные барьеры, анонимность субъектов и высокая латентность деяний существенно снижают эффективность классических правоохранительных механизмов.

В противовес этому неформальный социальный контроль представляет собой совокупность спонтанно возникающих и целенаправленно культивируемых социальных норм, ценностных ориентиров, моральных установок и поведенческих практик, которые обеспечивают устойчивость общественного порядка через механизмы внутренней саморегуляции индивидов и групп. В отличие от

формальных институтов, действующих по принципу «запрещено – наказано», неформальный контроль функционирует на уровне «принято – не принято», «опасно – безопасно», «допустимо – недопустимо», апеллируя к совести, здравому смыслу, репутационным рискам и социальному одобрению.

Принципиально важным для методологического анализа является различение девиантного явления как институционализированной системы (т. е. сложившейся криминальной экосистемы, включающей иерархию, специализацию и устойчивые связи) и девиантных отношений как первичных практик, отдельных актов отклоняющегося поведения, которые потенциально могут быть купированы на ранних стадиях с помощью средств социального контроля. Сущность неформального контроля в данном контексте заключается именно в предотвращении перехода спорадических девиантных отношений в системную, институционализированную девиантную структуру. Именно на этой логике строится современная модель профилактической работы в сфере киберпреступности, где приоритет отдается не столько постфактумному наказанию, сколько предварительному информированию, просвещению и формированию устойчивых навыков безопасного поведения.

Применительно к киберпреступности, неформальный социальный контроль обретает конкретные формы и методы, среди которых ключевое место занимает информационно-просветительская деятельность, направленная на повышение цифровой грамотности населения, развитие критического мышления при работе с контентом, а также внедрение культуры безопасного поведения в сети. Специфика цифровой среды накладывает на эти процессы особый отпечаток: информация здесь распространяется с беспрецедентной скоростью, охватывает глобальную аудиторию, обладает высокой степенью интерактивности и масштабируемости, что превращает медиа-коммуникации в мощнейший рычаг социального воздействия.

Однако нельзя не учитывать и серьезные ограничения, присущие неформальному контролю в цифровой среде. К ним, в первую очередь, относятся: фрагментарность и неполнота данных, доступных широкой общественности (что

затрудняет объективное восприятие угроз); асимметрия информации между профессиональными участниками рынка и рядовыми пользователями; а также потенциальный риск использования самих информационных технологий во вред обществу – например, для распространения фейков, манипуляции массовым сознанием или создания искусственной паники. Данные ограничения настоятельно требуют выработки сбалансированных, верифицированных и этически выверенных подходов к организации неформального контроля, где СМИ выступают не только транслятором, но и фильтром социально значимой информации.

Актуальная повестка государственной политики в сфере противодействия киберпреступности все более отчетливо смещается в сторону признания ключевой роли информирования как самостоятельной профилактической меры, а не лишь вспомогательного инструмента, сопровождающего репрессивные действия. Как подчеркнул заместитель Министра юстиции РФ Вадим Федоров, потенциал СМИ должен быть задействован для выстраивания в обществе принципиально новой культуры правосознания, причем делать это необходимо на опережение, упреждая преступные замыслы злоумышленников. Это означает, что медиа должны не просто констатировать факты совершения преступлений, но систематически, планомерно и доступно разъяснять гражданам механизмы мошенничества, алгоритмы распознавания угроз и правила самозащиты.

Особую значимость в этом контексте приобретает специализированное правовое просвещение с учетом психологической специфики киберпреступности. Как справедливо отмечает начальник отдела Генеральной прокуратуры РФ Олег Кипкаев, главное оружие современных киберпреступников – это не столько технический взлом, сколько умелое психологическое воздействие на человека, особенно на наиболее внушаемые и социально незащищенные группы, включая молодежь и пожилых людей. Задача СМИ, следовательно, состоит не в запугивании, а в спокойном, систематическом научении граждан распознавать манипулятивные техники, понимать природу фишинговых атак, отличать официальные уведомления от мошеннических предложений и, что самое важное, владеть четким, пошаговым алгоритмом действий в случае возникновения подозрений.

Ярким примером удачного формата информационного воздействия служат кампании, реализуемые через современные цифровые площадки с использованием меметичных и легко запоминающихся хештегов. Так, инициатива Генеральной прокуратуры под хештегом #КладиТрубку позволила в сжатые сроки охватить многомиллионную аудиторию в социальных сетях и мессенджерах, предложив простой и понятный рефлекторный алгоритм поведения при поступлении подозрительных звонков. Данный пример демонстрирует, как креативная подача и адаптация содержания к форматам новой медиасреды могут многократно усиливать эффективность профилактического посыла.

Однако информационная кампания не будет полноценной, если она ограничивается лишь общими призывами к бдительности. Как резонно заметил председатель Комитета Госдумы по информационной политике Сергей Боярский, «инструменты защиты у вас у всех под рукой, их нужно всего лишь включить». Задача СМИ заключается именно в том, чтобы донести до каждой категории граждан – от школьников до пенсионеров – не абстрактные лозунги, а практические, конкретные и адаптированные к уровню их цифровой компетенции инструменты: как настроить двухфакторную аутентификацию, как проверить подлинность сайта, как не передать код из СМС и куда обращаться в случае инцидента.

В 2025–2026 годах в Российской Федерации был принят и введен в действие комплекс законодательных актов, существенно расширяющих функциональные обязательства и одновременно полномочия СМИ в области противодействия киберугрозам. Эти нормативные изменения, с одной стороны, формально закрепляют ответственность медиа за достоверность распространяемой информации о киберпреступлениях и обязательность их участия в государственных профилактических кампаниях, а с другой – создают правовую базу для более тесного взаимодействия журналистского сообщества с правоохранительными структурами и специальными службами.

Практический опыт свидетельствует, что эффективность неформального социального контроля возрастает на порядок, когда между СМИ и правоохранительными органами устанавливаются устойчивые каналы оперативного обмена

информацией и совместной методической работы. Показательным примером здесь служат учебно-практические курсы для журналистов «Бастион-2026», проведенные в Амурской области при активном участии сотрудников Управления МВД России. В рамках этих курсов была реализована принципиально важная модель прямого обучения медиа-специалистов основам кибербезопасности.

Сотрудники отдела по борьбе с противоправным использованием информационно-коммуникационных технологий провели серию углубленных занятий, посвященных не только общим вопросам защиты устройств и каналов связи, но и конкретным тактикам противодействия фишинговым атакам, целевым взломам аккаунтов, а также методам выявления и нейтрализации дезинформационных атак, направленных на дискредитацию официальных источников. Особое внимание в программе курсов уделялось психологически корректным способам информирования граждан о существующих цифровых угрозах – таким, чтобы информация была воспринята адекватно, не провоцировала панических настроений и не порождала чувства беспомощности. Как справедливо подчеркивалось организаторами, «от цифровой грамотности корреспондента напрямую зависит сохранность источников информации, целостность редакционных массивов и, в конечном счете, безопасность многомиллионной аудитории». Значимость такого рода взаимодействия трудно переоценить в условиях лавинообразного роста киберугроз, когда объективное и взвешенное информационное поле становится критическим ресурсом национальной устойчивости.

Освещение криминальной тематики в СМИ всегда сопряжено с повышенной этической ответственностью, а в сфере киберпреступности эта ответственность приобретает новые, доселе не встречавшиеся измерения. Наиболее остро данная проблема стоит в сегменте криминально-правовых программ и специализированных репортажей, где систематически фиксируются нарушения базовых журналистских и правовых принципов. Среди наиболее распространенных этических дефицитов можно выделить: прямое нарушение запрета на идентификацию жертв, что приводит к их вторичной травматизации и нарушению права на частную жизнь; неконтролируемое распространение деструктивных элементов

контента (например, ссылок на фишинговые ресурсы в погоне за сенсационностью); непреднамеренную романтизацию образа киберпреступника как виртуозного «хакера-одиночки», противостоящего системе; а также использование пугающих, драматизированных формулировок, формирующих у аудитории чувство тотальной незащищенности и беспомощности.

Эти системные проблемы требуют не просто индивидуального осуждения, но институциональной рефлексии и выработки формализованных этических стандартов. В качестве практического решения предлагается разработка и имплементация специализированных рекомендаций для редакций СМИ по распространению информации о киберпреступлениях. Эти рекомендации должны включать: четкие критерии допустимой степени детализации сценариев мошенничества (во избежание превращения материалов в инструкции для подражателей); обязательные правила анонимизации и деидентификации жертв; строгие ограничения на использование мультимедийных элементов, воспроизводящих психологическое давление на зрителя; а также создание памяток для авторов и редакторов криминально-правовых программ, регламентирующих баланс между общественной значимостью информации и защитой индивидуальной безопасности.

Помимо этого, целесообразно внедрение механизмов общественно-профессионального аудита криминального контента, с участием как экспертов в области медиаэтики, так и специалистов-психологов, способных оценить долгосрочное воздействие материалов на различные возрастные и социальные группы. Только комплексный подход к этической регламентации позволит превратить СМИ из потенциального источника дезинформации и паники в надежного союзника государства и граждан в борьбе с цифровыми угрозами.

Проведенный анализ теоретических концепций, эмпирических данных и практических кейсов позволяет сформулировать ряд обобщающих выводов, имеющих как научное, так и прикладное значение.

Во-первых, неформальный социальный контроль представляет собой не просто желательное, но абсолютно необходимое дополнение к формально-правовым механизмам противодействия киберпреступности. Его уникальная

ценность заключается в способности воздействовать на досовершенный этап преступного поведения, формируя у граждан устойчивые внутренние барьеры и навыки самозащиты. Исключительно правовые меры, несмотря на их императивность, принципиально недостаточны в силу того, что девиантные отношения в цифровой среде глубоко вплетены в ткань повседневных неформальных практик, социальных норм и межличностных коммуникаций, которые не поддаются прямому нормативному регулированию.

Во-вторых, средства массовой информации занимают центральное, системообразующее место в архитектуре этого неформального контроля. Эффективность их деятельности, однако, не является автоматической и требует выстраивания стратегически продуманного, системного подхода, включающего регулярность тематических публикаций и эфиров, создание специализированных рубрик и порталов, разработку и распространение доступных памяток для разных целевых аудиторий, а также постоянное профессиональное взаимодействие с правоохранительными органами на основе принципов доверия и взаимной методической поддержки. Адаптация контента под различные социальные и возрастные когорты должна стать аксиомой медиа-планирования в этой сфере.

В-третьих, перспективным и наиболее результативным направлением развития системы противодействия киберпреступности является глубокая интеграция формальных (правоохранительных, судебных, регулирующих) и неформальных (медийных, просветительских, культурно-нормативных) механизмов в единую, синергийную систему. Такая интеграция предполагает не просто параллельное существование двух треков работы, а их органическое взаимопроникновение, где каждое правовое решение находит свое информационное и разъяснительное сопровождение, а каждая просветительская кампания подкрепляется реальными юридическими гарантиями защиты граждан.

Реализация предложенных направлений – от законодательного закрепления стандартов медиаучастия до внедрения этических кодексов и обучающих программ для журналистов – позволит существенно повысить эффективность неформального социального контроля над киберпреступностью. Это, в свою

очередь, внесет весомый вклад в защиту конституционных прав и законных интересов граждан в условиях все более усложняющейся цифровой среды, где скорость реакции и качество информации становятся решающими факторами безопасности. Дальнейшие исследования в этой области могут быть направлены на разработку количественных методик оценки эффективности различных медийных форматов, а также на изучение долгосрочных эффектов информационно-просветительских кампаний на трансформацию массового правосознания.

***Список литературы***

1. Ardelyanova Ya. Directions and measures of informal social control of corruption relations / Ya. Ardelyanova // The Scientific Heritage. – 2025. – №170. – URL: https://cyberleninka.ru/article/n/directions-and-measures-of-informal-social-control-of-corruption-relations (date of access: 03.06.2026).

2. В ГД рассказали, как будет работать закон о профилактике киберпреступлений. – URL: https://news.mail.ru/society/61987321/ (дата обращения: 10.06.2026).

3. Правительство решило установить слежку за подростками в интернете. – URL: https://www.moscowtimes.ru/2026/05/05/pravitelstvo-reshilo-ustanovit-slezhku-za-podrostkami-v-internete (дата обращения: 10.06.2026).

4. В Амурской области полицейские провели занятия для журналистов на курсах «Бастион-2026». – URL: https://news.rambler.ru/other/54387645-v-amurskoy-oblasti-politseyskie-proveli-zanyatiya-dlya-zhurnalistov-na-kursah-bastion-2026/ (дата обращения: 10.06.2026).

5. В Благовещенске полицейские провели занятия для журналистов на курсах «Бастион-2026». – URL: https://pressamagdagachi.ru/news/2026/06/03/v-blagoveschenske-politseyskie-proveli-zanyatiya-dlya-zhurnalistov-na-kursah-bastion-2026/ (дата обращения: 10.06.2026).

6. В российском интернете создадут кибердружины и запустят медиапатрули. – URL: https://www.fontanka.ru/2026/05/05/76854321/ (дата обращения: 10.06.2026).

7. Заседание Общественного совета при Роскомнадзоре. – URL: https://www.law.msu.ru/news/zasedanie-obshhestvennogo-soveta-pri-roskomnadzore (дата обращения: 05.06.2026).

8. Алгоритмы самозащиты: роль СМИ в схватке с кибермошенничеством. – URL: https://ruj.ru/news/algorithmy-samozashchity-rol-smi-v-skhvatke-s-kibermoshennichestvom/ (дата обращения: 15.04.2026).

9. С. Перминов: В борьбе с кибермошенниками роль СМИ – всеохватное объяснение. – URL: http://council.gov.ru/events/features/154321/ (дата обращения: 15.04.2026).

10. Депутат Толмачев рассказал о новых инициативах в сфере кибербезопасности. – URL: https://www.pnp.ru/social/deputat-tolmachev-rasskazal-o-novykh-inicziativakh-v-sfere-kiberbezopasnosti.html (дата обращения: 10.06.2026).