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

АКТУАЛЬНЫЕ ПРОБЛЕМЫ СОЦИАЛЬНОГО КОНТРОЛЯ НАД КИБЕРПРЕСТУПНОСТЬЮ И ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ МЕХАНИЗМОВ СОЦИАЛЬНО-ПРАВОВОГО РЕГУЛИРОВАНИЯ В РОССИИ

Аннотация: *в статье проводится комплексный анализ актуальных проблем социального контроля над киберпреступностью в Российской Федерации. Рассматривается феноменология современных киберугроз, включая использование искусственного интеллекта, атаки на критическую информационную инфраструктуру и модели преступности «как услуга» (CaaS). Исследуется текущее состояние правового регулирования и деятельности правоохранительных органов, выявляются ключевые пробелы, такие как недостаточная скорость адаптации законодательства, проблемы с квалификацией составов преступлений и сложности международного сотрудничества. На основе анализа предлагается комплекс мер по совершенствованию социально-правового регулирования, включающий развитие специализированных подразделений, усиление публично-частного партнерства, внедрение прорывных технологий и реализацию масштабных программ по повышению цифровой грамотности населения. Особое внимание уделяется необходимости построения комплексной системы защиты жертв киберпреступлений.*

Ключевые слова: *киберпреступность, социальный контроль, правовое регулирование, кибербезопасность, защита жертв, правоохранительные органы, цифровая гигиена, Российская Федерация.*

Цифровая трансформация, охватившая все сферы общественной жизни в начале XXI века, привела к фундаментальным изменениям в структуре социальных взаимодействий, экономических отношений и механизмах государственного

управления. Наряду с неоспоримыми благами, которые принесли информационно-коммуникационные технологии, возникло и стремительно развивается новое, виртуальное пространство для противоправной деятельности. Киберпреступность представляет собой один из наиболее динамичных и социально опасных вызовов современности, требующий адекватных мер социального и правового контроля, способных не только реагировать на уже совершённые деяния, но и работать на упреждение, предотвращая переход девиантных отношений в институционализированную преступную систему.

Традиционные подходы к противодействию преступности, сложившиеся в эпоху доминирования физических коммуникаций и территориальной юрисдикции, зачастую оказываются неэффективными в условиях анонимности, трансграничности и высокой технологичности киберугроз. В России масштабы и сложность этой проблемы стремительно нарастают, что актуализирует необходимость научного осмысления существующих вызовов и поиска путей оптимизации государственной и общественной реакции. Как справедливо отмечает доктор социологических наук, профессор Ю.Ю. Комлев, «цифровые технологии в жизнедеятельности современного человека привели не только к позитивным, но и к негативным последствиям. Среди них наибольшие риски представляет киберпреступность, темпы роста которой возрастают с каждым годом». Целью данной статьи является выявление ключевых проблем социального контроля над киберпреступностью в России и оценка возможностей применения комплексных механизмов социально-правового регулирования для их решения, с особым акцентом на кадровое обеспечение правоохранительных органов и развитие специализированных подразделений.

Современная киберпреступность в России характеризуется быстрой эволюцией и диверсификацией, принимая всё более изощрённые и технологически оснащённые формы. К числу наиболее актуальных угроз относятся следующие феномены.

Использование искусственного интеллекта (ИИ). Киберпреступники начали применять технологии ИИ для создания убедительных фишинговых сообщений,

которые имитируют стиль письма конкретных людей и обладают безупречной грамматикой, что значительно усложняет их обнаружение традиционными средствами антивирусной защиты. Кроме того, ИИ используется для автоматизации и масштабирования атак, например, для сканирования уязвимостей или одновременного развертывания вредоносных программ по множеству целей. Как подчеркивает Председатель Следственного комитета Российской Федерации А.И. Бастрыкин, «самым новым вызовом для следователей является применение злоумышленниками искусственного интеллекта для совершения противоправных действий. Например, для подделки голоса и изображения человека при телефонных разговорах с родственниками с целью хищения средств».

Атаки на критическую информационную инфраструктуру (КИИ). Наблюдается устойчивый рост целенаправленных атак на объекты энергетики, здравоохранения, транспорта и агропромышленного комплекса. Например, в 2025 году была зафиксирована волна атак группировки Cloud Atlas на российские предприятия АПК с использованием уязвимостей в Microsoft Office. Подобные атаки несут риск не только значительных финансовых потерь, но и дестабилизации жизнеобеспечения целых регионов, что переводит их в разряд угроз национальной безопасности.

Эволюция программ-вымогателей. Традиционные схемы вымогательства, основанные на блокировке доступа к данным, сменились более изощрёнными моделями с двойным вымогательством, когда злоумышленники не только шифруют данные жертвы, но и похищают их, угрожая последующей публикацией в случае неуплаты выкупа. Это создаёт дополнительное психологическое давление на пострадавших и повышает вероятность выплаты требований.

Рост мошенничеств с использованием социальной инженерии. По данным на 2025 год, около 35 % попыток обмана приходится на звонки от лжесотрудников Центрального банка и правоохранительных органов. Также широко распространены схемы под видом сотрудников служб доставки (20 %) и несанкционированный перевыпуск SIM-карт (15 %). Эти цифры свидетельствуют о том, что основным уязвимым звеном в системе кибербезопасности остаётся человеческий

фактор, а точнее – недостаточный уровень критического мышления и цифровой грамотности населения.

Преступность как услуга (CaaS – Crime-as-a-Service). Набирает обороты модель, при которой киберпреступники предоставляют друг другу в аренду хакерские инструменты, инфраструктуру и услуги, что значительно снижает «порог входа» в криминальную деятельность и масштабирует угрозу. Как отмечает профессор Комлев, анализируя этот тренд, «динамичный криминальный мир быстро реагирует на технологические изменения», и киберпреступность «всё больше направлена в отношении многочисленных частных пользователей социальных сетей и Интернета».

Анализ текущей ситуации позволяет выявить ряд системных проблем, препятствующих эффективному противодействию киберпреступности в России. Эти проблемы носят не только правовой, но и организационный, технологический и социальный характер.

Правовые пробелы и отставание законодательства. Действующая глава 28 Уголовного кодекса РФ (ст. 272–274), принятая в иной технологической реальности, не в полной мере охватывает спектр современных киберугроз. Отсутствуют чёткие законодательные определения таких понятий, как «киберпреступность», «компьютерная атака», «информационная угроза», что приводит к сложностям в квалификации преступлений и формировании единообразной судебной практики. Как справедливо отмечает Председатель СК России, «принцип внесения изменений должен быть от общего к частному. Первоочередной инициативой является проработка законопроекта по дополнению общей части Уголовного кодекса новым отягчающим обстоятельством – совершение преступления с использованием информационно-коммуникационных технологий, включая технологии искусственного интеллекта».

Недостаточная эффективность правоохранительной системы. Расследование киберпреступлений сопряжено с трудностями сбора и фиксации цифровых доказательств, которые отличаются «хрупкостью» и могут быть легко оспорены в суде. Зачастую привлекаемые специалисты не обладают достаточной

квалификацией для раскрытия сложных технических деталей преступлений. Несмотря на создание в декабре 2024 года специализированного отдела по расследованию киберпреступлений в составе Главного следственного управления СК России, проблема межведомственного взаимодействия и кадрового дефицита остаётся острой. На региональном уровне, как свидетельствует опыт Мурманской области, подразделения по борьбе с киберпреступностью созданы сравнительно недавно – во исполнение Указа Президента РФ от 30 сентября 2022 года, и процесс накопления экспертизы находится в начальной стадии.

Трансграничный характер угроз. Большинство кибератак совершается из-за рубежа, что создаёт непреодолимые процессуальные и политические барьеры для оперативного расследования и привлечения виновных к ответственности. Как подчёркивает руководство СК России, «учитывая нежелание представителей ряда зарубежных мессенджеров, социальных сетей и других агрегаторов информации взаимодействовать с российскими правоохранительными органами, на их помощь рассчитывать не приходится». Механизмы международного сотрудничества, такие как Конвенция о киберпреступности Совета Европы, в текущих геополитических условиях работают не в полную силу, хотя Россия активно участвует в разработке альтернативной конвенции ООН против киберпреступности.

Низкий уровень цифровой грамотности населения. Значительная часть успеха киберпреступников строится на манипулировании пользователями, которые пренебрегают правилами «кибергигиены»: используют простые пароли, переходят по подозрительным ссылкам, не обновляют программное обеспечение и бездумно делятся личной информацией в социальных сетях. Профессор Комлев в своих исследованиях обращает внимание на феномен «кибервиктимизации», подчёркивая, что «пользователи интернета, социальных сетей и цифровых платежных систем – основные жертвы пандемии киберпреступности».

Одним из ключевых направлений повышения эффективности противодействия киберпреступности является развитие специализированных подразделений и, что особенно важно, подготовка высококвалифицированных кадров для работы в этой сфере. Данная проблематика находится в центре научных

интересов профессора Ю.Ю. Комлева, который предлагает концептуально новые подходы к решению кадрового дефицита.

Как отмечает профессор Комлев, «на мировом рынке труда по мере роста киберпреступности сложился высокий и устойчивый спрос на подготовку специалистов по кибербезопасности, по розыску киберпреступников и расследованию киберпреступлений – киберполицейских. Однако подготовленных специалистов такого рода в России хронически не хватает». Это дефицит имеет как количественное, так и качественное измерение. В то время как крупный бизнес активно привлекает IT-специалистов с медианной зарплатой 150 000 рублей и выше, в органах внутренних дел, по экспертным оценкам, средняя зарплата оперативного сотрудника не намного превышает 60 000 рублей. В таких условиях, как резюмирует профессор Комлев, «закрепить специалиста по кибербезопасности – выпускника гражданского вуза в правоохранительных органах практически нереально. Надо готовить свои ведомственные кадры».

Выход из этой ситуации профессор Комлев видит в создании междисциплинарных образовательных программ, интегрирующих правовые, поведенческие и технологические знания. Он обосновывает необходимость подготовки киберполицейских в рамках магистерских программ с профилем «расследование цифровых преступлений». Такая программа должна обеспечить синтез фундаментальных знаний в области цифровых технологий, методологии защиты цифровой информации, криптографии, электронной коммерции, а также специальных дисциплин, изучающих кибердевиантность и киберпреступность, документирование цифровых следов и методику расследования.

Принципиально важным, по мнению профессора Комлева, является использование ведомственной образовательной системы МВД России, где уже сформирован фундамент правовых и девиантологических исследований, с привлечением специалистов из IT-сферы и правоприменительной практики. Такой подход позволит готовить специалистов, которые «хорошо разбираются в праве, в девиантных практиках, цифровых технологиях, способах совершения деликтов, расследования и противодействия цифровым преступлениям». В качестве успешных

примеров он приводит программы подготовки специалистов по кибербезопасности в Московском и Санкт-Петербургском университетах МВД России, а также недавнюю инициативу по подготовке медиаполицейских в Российской академии народного хозяйства и государственной службы для выявления деструктивных материалов в интернете.

В 2025–2026 годах эта концепция получила дальнейшее развитие в связи с принятием комплекса законодательных мер, закрепляющих роль профильных подразделений в системе противодействия киберпреступности. В Следственном комитете, как сообщил А.И. Бастрыкин, создан специализированный отдел, «обладающий профессиональными кадрами и необходимой программно-аппаратной базой», где внедрён инструментарий для аналитики больших объёмов данных, исследования криптовалютных транзакций и преодоления систем шифрования.

Для построения эффективной системы контроля над киберпреступностью необходим комплексный подход, сочетающий правовые, организационные, технологические и социальные меры.

Совершенствование законодательной базы. Требуется внесение изменений в Уголовный и Уголовно-процессуальный кодексы РФ, направленных на детализацию составов киберпреступлений, закрепление современных правил работы с цифровыми доказательствами и криминализацию новых видов противоправной деятельности (например, криптоджекинга, массового создания ботнетов, использования технологий искусственного интеллекта как отягчающего обстоятельства). Как справедливо указывает А.И. Бастрыкин, также необходимо проанализировать отдельные составы преступлений, чтобы понять, «где применение таких технологий преступниками представляет наиболее высокую общественную опасность».

Развитие кадрового потенциала. Целесообразно усилить потенциал киберполиции и других правоохранительных органов путём создания профильных учебных программ, курсов переподготовки и привлечения специалистов из частного сектора. Опыт таких стран, как США, где принят специализированный

Cybersecurity Act, свидетельствует о важности концентрации экспертизы и создания национальных центров по борьбе с киберпреступностью.

Публично-частное партнёрство. Активное усиление публично-частного партнёрства, взаимодействие государства с компаниями в сфере информационной безопасности, телекоммуникаций и финансов позволит обмениваться данными об угрозах в режиме, близком к реальному времени, и оперативно блокировать мошеннические схемы. Как отмечается в утверждённой Правительством РФ в августе 2025 года концепции противодействия киберпреступности, необходимо активное использование цифровых двойников, искусственного интеллекта и мобильных приложений для прогнозирования и пресечения кибератак.

Защита жертв киберпреступлений и повышение цифровой грамотности. Необходимо создание удобных и доступных механизмов для пострадавших, включая упрощённую процедуру подачи заявлений и получение психологической помощи. Профессор Комлев подчёркивает, что профилактика кибердевиантности должна строиться «в контексте формирования основ цифрового общества и цифрового гражданства», что предполагает вовлечение молодёжи в цифровую культуру через образовательные программы.

Актуальные проблемы социального контроля над киберпреступностью в России носят комплексный характер и связаны с быстрой эволюцией угроз, несовершенством законодательства, недостаточной технической оснащённостью правоохранительных органов, кадровым дефицитом и низкой цифровой культурой населения. Как показывает научный анализ, проведённый профессором Ю.Ю. Комлевым, одним из наиболее перспективных направлений решения кадровой проблемы является внедрение междисциплинарных магистерских программ по подготовке киберполицейских в ведомственной образовательной системе, позволяющих синтезировать правовые, технологические и девиантологические знания.

Возможности для полноценного применения механизмов социально-правового регулирования заключаются в синтезе жёстких правовых мер, направленных на ужесточение ответственности и совершенствование процедур

расследования, с гибкими социальными инструментами, такими как публично-частное партнёрство, образовательные инициативы и внедрение прорывных технологий. Только комплексный и опережающий подход, учитывающий как формальные институциональные механизмы, так и неформальные практики социального контроля, позволит построить в России устойчивую систему противодействия киберпреступности, обеспечивающую защиту как интересов государства и бизнеса, так и прав рядовых граждан. Цифровой социальный контроль, по справедливому замечанию профессора Комлева, должен опираться «на цифровые технологии и искусственный интеллект, что делает их адекватными вызовам XXI века».

Список литературы

1. Киберпреступность и киберконфликты: Россия // Tadviser. – URL: https://www.tadviser.ru/index.php/Статья:Киберпреступность_и_киберконфликты_:_Россия (дата обращения: 18.11.2025).

2. 13 простых правил, которые помогут вам не стать жертвой киберпреступления. – URL: https://agapovka.ru/pravoohranitelnye-struktury/stranica-prokurora/prokuror-razyasnyaet/13-prostyh-pravil-kotorye-pomogut-vam-ne-stat-zhertvoi-kiberprestupleniya (дата обращения: 18.11.2025).

3. Черенцов Р.С. Проблемы правового регулирования киберпреступности в современной России / Р.С. Черенцов // Актуальные исследования. – 2025. – №21(256). – Ч. III. – С. 54–56. EDN TAKFKN

4. Что такое киберпреступность и как защитить себя? // Kaspersky.ru. – URL: https://www.kaspersky.ru/resource-center/threats/what-is-cybercrime (дата обращения: 18.11.2025).

5. Федеральный закон «Уголовный кодекс Российской Федерации» №63-ФЗ от 13.06.1996 (ред. от 21.04.2025). – Ст. 272–274.

6. Комлев Ю.Ю. От цифровизации социума и киберпреступности к подготовке киберполицейских / Ю.Ю. Комлев // Вестник экономики, права и социологии. – 2025. – №2. – С. DOI 10.24412/1998-5533-2025-2-378-382. EDN FREOSN