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

ПОЗИТИВНАЯ ДЕВИАЦИЯ В ПРАВОВОМ РЕГУЛИРОВАНИИ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ: ОТ ДОГОНЯЮЩЕЙ РЕАКЦИИ К ОПЕРЕЖАЮЩЕМУ КОНТРОЛЮ

Аннотация: *статья посвящена исследованию феномена позитивной девиации в правовом регулировании противодействия киберпреступности в Российской Федерации в период 2017–2025 годов. В работе обосновывается, что российская правовая система демонстрирует сознательное, конструктивное отклонение от устаревающих правовых норм, направленное на создание более эффективных и адекватных цифровой эпохе правовых конструкций. Автор анализирует эволюцию международно-правового регулирования – от Будапештской конвенции Совета Европы 2001 года к Ханойской конвенции ООН против киберпреступности (2024–2025), а также национальную стратегию противодействия киберпреступности, включая Концепцию государственной системы противодействия преступлениям, совершаемым с использованием ИКТ (2024) и План мероприятий по её реализации (2025).*

В статье рассматриваются ключевые проблемы правоприменительной практики: сложности квалификации киберпреступлений, дефицит квалифицированных кадров для киберполиции, отсутствие процессуального статуса данных, полученных с использованием систем искусственного интеллекта, а также низкая эффективность межведомственного взаимодействия. На основе анализа научных позиций профессора Ю.Ю. Комлева, П.А. Скобликова, А.Ю. Сергеева, О.В. Широковой, П.С. Швыряева и Е.В. Фомина предлагаются конкретные направления совершенствования законодательства, включая разработку Федерального закона «О базовых гарантиях прав жертв киберпреступлений» и внесение изменений в Уголовно-процессуальный кодекс РФ в части легализации

использования технологий искусственного интеллекта в следственной деятельности.

Особое внимание уделяется подготовке специализированных кадров для киберполиции, обосновывается необходимость внедрения междисциплинарных магистерских программ в ведомственной образовательной системе МВД России. Автор приходит к выводу, что интеграция формальных правовых механизмов и неформальных практик социального контроля с использованием потенциала средств массовой информации и цифровых технологий является наиболее перспективным направлением построения устойчивой системы противодействия киберпреступности.

Ключевые слова: *киберпреступность, позитивная девиация, социальный контроль, правовое регулирование, Конвенция ООН против киберпреступности, Ханойская конвенция, Будапештская конвенция, искусственный интеллект, киберполиция, цифровые доказательства, защита жертв, кибердевиантность, цифровая грамотность, уголовно-процессуальное законодательство, межведомственное взаимодействие, подготовка кадров, цифровая трансформация, правоприменительная практика, профилактика киберпреступлений, неформальный социальный контроль.*

В эпоху цифровой трансформации, когда, по экспертным оценкам, до 40% всех преступлений совершается с использованием информационно-коммуникационных технологий, традиционные правовые механизмы оказываются в положении «вечно догоняющих». Российская правовая система, столкнувшись с этим вызовом, демонстрирует феномен позитивной девиации – сознательного, конструктивного отклонения от устоявшихся, но устаревающих норм в целях создания более эффективных и адекватных времени правовых конструкций. Это отклонение направлено не на разрушение правопорядка, а на его усиление через адаптацию к новой цифровой реальности.

Как отмечает доктор социологических наук, профессор Ю.Ю. Комлев, «цифровые технологии в жизнедеятельности современного человека привели не

только к позитивным, но и негативным последствиям. Среди них наибольшие риски представляет киберпреступность, темпы роста которой возрастают с каждым годом». Профессор Комлев подчеркивает, что в современной науке сформировалось новое предметное поле цифровой девиантологии, которое лежит «на пересечении криминологии как социологической науки о преступности, цифровой социологии, традиционной позитивистской и постмодернистской юриспруденции, психологии, педагогики, семиотики, теории масс-медиа и других наук». В своих исследованиях он акцентирует внимание на дуализме и контекстуальности социальной нормы и девиантности, обосновывая необходимость интегративного исследования различных проявлений девиантности и преступности на основе дополнительности объективистских и субъективистских интерпретаций социальной нормы. Предложенный исследовательский ракурс, по его убеждению, «обладает практически ценным эвристическим потенциалом при изучении кибердевиантности и киберпреступности для совершенствования моделей социального контроля над ними в новом мире».

В контексте цифровой девиантологии профессор Комлев определяет кибердевиантность как «множество проявлений девиантного поведения в киберпространстве Интернета, состоящих в нарушении социальных норм с использованием компьютеров, цифровых технологий, обращенных против компьютерных систем, социальных сетей и их конечных пользователей» [5]. При этом он обращает внимание на принципиальное обстоятельство: «в настоящее время кибердевиантность в целом… все больше направлена в отношении многочисленных частных пользователей социальных сетей и Интернета». Пользователи интернета, социальных сетей и цифровых платежных систем становятся основными жертвами «пандемии киберпреступности», что актуализирует проблему кибервиктимизации и требует выработки эффективных механизмов защиты прав граждан в цифровой среде.

А.Ю. Сергеев и О.В. Широкова в своем исследовании мошенничества в цифровом обществе отмечают, что «цифровизация социальных отношений создает принципиально новую среду для противоправной деятельности, где

традиционные механизмы социального контроля утрачивают свою эффективность». Авторы подчеркивают, что мошенничество в цифровом обществе приобретает системный характер, а его профилактика требует не только правовых, но и социально-психологических мер воздействия на потенциальных жертв и преступников.

П.А. Скобликов обращает внимание на фундаментальную проблему оценки реальных масштабов киберпреступности. В своей работе он выдвигает и обосновывает гипотезу о том, что «фактические масштабы киберпреступности многократно превышают официально регистрируемые показатели». По его мнению, «правоприменительные органы недостаточно ориентированы на своевременное и тщательное выявление преступлений, совершаемых с использованием ИКТ», а сообщения о таких преступлениях «часто не получают немедленной процессуальной реакции и во многих случаях рассматриваются спустя длительное время после подачи, как правило, сотрудниками, не обладающими необходимыми навыками, криминалистическими инструментами и процессуальными полномочиями». В результате, как резюмирует Скобликов, «субъекты уголовной политики не имеют точного представления о ситуации в этой сфере контроля над преступностью», что делает невозможным принятие обоснованных управленческих решений.

Особую значимость приобретает разработанная П.А. Скобликовым система критериев оценки эффективности работы подразделений по противодействию киберпреступности. Он предлагает, чтобы «выявление таких преступлений поощрялось, даже если виновные лица не установлены», а «к дополнительным преференциям должны приводить своевременное выявление и фиксация улик, получение оперативно значимой информации, что может в дальнейшем способствовать установлению виновных, их задержанию, возмещению ущерба».

В рамках диссертационного исследования П.С. Швыряева, защищенного в МГУ имени М.В. Ломоносова, киберпреступность определяется как «незаконная деятельность по поиску и эксплуатации социальных и технических уязвимостей социо-цифровой системы». Автор обосновывает, что киберпреступность

возникает и активизируется «на стыке технического и социального, в условиях дисбаланса между ними, возникающего, когда происходит освоение обществом новых цифровых технологий». Анализ пятилетней динамики развития киберпреступности в России, проведенный Швыряевым, позволяет сделать вывод о «критическом росте значения социальных факторов киберпреступности»: «по мере нарастания технических возможностей защиты фокус внимания киберпреступного сообщества сместился в сторону человека – к самому слабому звену в системе защиты от киберугроз». Эффективная стратегия противодействия, по мнению автора, должна быть «направлена на создание такого состояния системы, в котором вероятность эксплуатации уязвимостей минимизирована, а порог проникновения сквозь защитный барьер системы высок и сложен», и базироваться на принципах «системности, долговременности, непрерывности, упреждающего характера».

Е.В. Фомин в своих работах, посвященных определению понятийного аппарата киберпреступности, подчеркивает сложность и дискуссионность терминологических подходов. Он отмечает, что в девиантологии «многие понятия не устоялись, что определяет актуальность предложенных определений и подходов». Фомин рассматривает соотношение понятий «компьютерная преступность», «киберпреступность» и «интернет-преступность», обосновывая необходимость их четкого разграничения для целей правоприменения и статистического учета. По его мнению, «компьютерная преступность» может рассматриваться в узком и широком смыслах, причем в узком смысле она шире по объему и содержанию таких понятий, как «киберпреступность» и «интернет-преступность».

П.А. Скобликов, в свою очередь, критически оценивает попытки определения киберпреступности через категорию «сфера высоких технологий», указывая, что такое понимание «чрезмерно сужает анализируемое понятие и лишает его практического смысла». Он подчеркивает, что отступление от формального определения размывает содержание киберпреступности и создает трудности для правоприменительной практики.

Таким образом, анализ научной литературы показывает, что проблематика противодействия киберпреступности находится в фокусе внимания многих исследователей, при этом остаются дискуссионными как определение самого понятия «киберпреступность», так и оценка эффективности существующих механизмов социального и правового контроля. Концепция позитивной девиации, предложенная в данной статье, позволяет рассматривать эволюцию правового регулирования в этой сфере как сознательное и конструктивное отклонение от устаревающих норм, направленное на адаптацию правовой системы к вызовам цифровой эпохи.

Обзор основных правовых документов за период 2017–2025 годов показывает, что к 2025 году сформировался многоуровневый правовой каркас противодействия киберпреступности, сочетающий международные инициативы, национальную стратегию и конкретные правоприменительные нормы. Этот процесс представляет собой классический пример позитивной девиации в сфере международного права, где отдельные государства сознательно отклоняются от устаревающих международных соглашений в пользу более адекватных современным реалиям правовых конструкций.

На международном уровне ключевым событием стало принятие Конвенции ООН против киберпреступности, получившей неофициальное название «Ханойская конвенция». Инициированный Россией в 2017 году проект был окончательно принят Генеральной Ассамблеей ООН в декабре 2024 года и подписан 73 государствами, включая Россию, в октябре 2025 года. Как отмечает Совет по развитию гражданского общества и правам человека, инициатива России по созданию универсального механизма привлечения к ответственности за преступления в сфере ИКТ была услышана и проработана на международном уровне. Еще в 2017 году российские дипломаты указали на неприемлемость информационной гегемонии западных стран, возможности вмешательства зарубежных спецслужб в работу компьютерных сетей других государств и предложили разработать альтернативу Конвенции Совета Европы о преступности в сфере компьютерной информации 2001 года – глобальную конвенцию ООН.

Этот документ стал ответом на ограниченность действовавшей с 2001 года Будапештской конвенции Совета Европы, которую многие страны, включая Россию, Китай и Индию, воспринимали как «нерепрезентативную» и чрезмерно привязанную к западным правовым подходам. Как отмечает Генеральный прокурор России Александр Гуцан, конвенция «построена на принципах равенства всех государств, а также принципах невмешательства в их внутренние дела». Показательно, что большинство стран мира разделяют российские подходы, сознают общую ответственность за реализацию принципа мирного сосуществования в информационном пространстве на основе уважения суверенитета, национального законодательства и традиций отдельных государств. Это, кстати, принципиальное отличие Конвенции ООН от Будапештской конвенции, которая, по мнению экспертов, «фактически легитимизировала право США без уведомления властей других стран вторгаться в их информационное пространство для сбора цифровых улик».

Ханойская конвенция закрепила принцип равенства государств-участников и создала рамки для оперативной правовой помощи, экстрадиции и, что критически важно, обязанности стран разрабатывать программы компенсации ущерба и реабилитации жертв киберпреступлений. Как подчеркнули представители Интерпола, «Конвенция обеспечивает прочную правовую и оперативную основу для скоординированных глобальных действий по борьбе с киберпреступностью, способствует гармонизации криминализации киберпреступлений, устанавливает процессуальные правила обмена электронными доказательствами и укрепляет международное сотрудничество в области профилактики и технической помощи».

Ключевое идеологическое различие между Будапештской и Ханойской конвенциями лежит в подходах к запуску расследований. Будапештская конвенция требовала предоставления доказательств «экстремизма» или «терроризма» на начальном этапе, что могло использоваться для политического давления. Ханойская конвенция, продвигаемая Россией, предлагает отталкиваться от собранных данных и косвенных признаков, что является более гибким и технологичным

подходом, соответствующим логике оперативно-розыскной деятельности. Это уточнение формулы международной правовой помощи можно считать прямой позитивной девиацией, направленной на деполитизацию сотрудничества.

В контексте международно-правового регулирования профессор Комлев обращает внимание на необходимость системного подхода к изучению киберпреступности как формы девиантного поведения. Он подчеркивает, что «в девиантологии многие понятия не устоялись, что определяет актуальность предложенных определений и подходов». Это методологическое замечание имеет прямое отношение к международному нормотворчеству: неопределенность ключевых понятий создает риски неэффективности правовых механизмов и требует постоянной рефлексии и уточнения дефиниций.

Е.В. Фомин также обращает внимание на сложность терминологических определений, отмечая, что отождествление таких понятий, как «киберпреступность», «компьютерная преступность» и «интернет-преступность», «размывает содержание киберпреступности» и создает трудности для правоприменительной практики.

На национальном стратегическом уровне основополагающим документом выступила Концепция государственной системы противодействия преступлениям, совершаемым с использованием ИКТ, утвержденная распоряжением Правительства РФ от 30 декабря 2024 года №4154-р. Согласно документу, одной из важных частей государственной системы должна стать специализированная цифровая платформа, обеспечивающая оперативный обмен информацией между правоохранительными органами, Центральным банком, кредитными организациями и операторами связи для установления всех обстоятельств и лиц, причастных к мошенническим действиям.

Концепция также предусматривает создание механизма оперативной приостановки операций с денежными средствами, использовавшимися в преступной деятельности, и совершенствование уголовного законодательства, в котором должны появиться новые определения видов преступлений, совершённых с использованием информационно-коммуникационных технологий. Особое

внимание уделяется повышению уровня осведомлённости граждан, в первую очередь пожилых, о методах мошенников и способах защиты от их действий. Для этого предлагается размещать социальную рекламу, цель которой – сформировать у граждан цифровую грамотность. К участию в такой социальной рекламе необходимо привлекать известных представителей культуры, науки и информационного сообщества.

Практическим воплощением концепции стало Распоряжение Правительства РФ от 14 августа 2025 года №2207-р, утвердившее детальный план мероприятий. Этот план синхронизировал работу всех ведомств (МВД, ФСБ, Минцифры, Банк России и др.) и сместил акцент с чистого преследования преступников на комплексную защиту граждан, включив меры по профилактике, повышению цифровой грамотности и техническому противодействию мошенникам. План 2025 года меняет расплывчатые формулировки о «необходимости взаимодействия» на конкретные поручения и сроки. Например, он предписывает проработать вопрос об обязанности операторов связи и интернет-провайдеров в автоматическом режиме уведомлять правоохранительные органы о признаках преступлений, а также интегрировать во все основные государственные и банковские приложения модули обязательного информирования граждан об угрозах. Это переход от рекомендации к императиву, возложение прямой ответственности на цифровых посредников.

В уголовном и уголовно-процессуальном праве базой остаются статьи 272–274 УК РФ (глава 28 «Преступления в сфере компьютерной информации»), криминализирующие неправомерный доступ, создание вредоносных программ и нарушение правил эксплуатации. Однако динамика преступности (мошенничество, кибертравля, груминг) постоянно требует их интерпретации и дополнения. Важным шагом стало введение уголовной ответственности для «дропперов» (денежных мулов) – лиц, предоставляющих преступникам свои банковские карты или счета для отмывания средств, что ранее было слабым звеном в цепочке расследования.

Анализ документов показывает отчетливый тренд на уточнение и расширение правовых дефиниций, движимый необходимостью закрывать возникающие правовые пробелы и адаптироваться к новым тактикам злоумышленников. Если изначально нормы были сфокусированы на защите компьютерной информации и имущественных прав (хищение денег), то к 2025 году в поле зрения законодателя и правоприменителя попали нематериальные блага. В официальных разъяснениях и планах мероприятий наравне с мошенничеством фигурируют кибербуллинг, киберпреследование (сталкинг) и кибергруминг – действия, направленные на причинение психологического вреда, особенно несовершеннолетним. Это отражает понимание, что вред от киберпреступности не сводится к финансовым потерям.

Как отмечает П.С. Швыряев, современные масштабы и последствия киберпреступности – это «симптом перехода преступности в киберпространство и ее превращения в одного из основных бенефициаров цифровизации, при одновременном нарастании рисков и угроз для других сторон этого процесса». Этот вывод подтверждает необходимость комплексного подхода к противодействию, учитывающего как технические, так и социальные аспекты проблемы.

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 высокой оплатой труда, в органах внутренних дел

закрепить специалиста по кибербезопасности – выпускника гражданского вуза практически нереально. Как резюмирует профессор Комлев, «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 сформирован фундамент правовых, девиантологических исследований и знаний» 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.

В 2025–2026 годах эта концепция получила дальнейшее развитие в связи с принятием комплекса законодательных мер, закрепляющих роль профильных подразделений в системе противодействия киберпреступности. Концепция государственной системы противодействия преступлениям, совершаемым с использованием ИКТ, прямо предусматривает создание специальных подразделений для расследования такого рода преступлений. В Следственном комитете создан специализированный отдел, обладающий профессиональными кадрами и необходимой программно-аппаратной базой, где внедрен инструментарий для

аналитики больших объемов данных, исследования криптовалютных транзакций и преодоления систем шифрования.

П.А. Скобликов, анализируя проблему кадрового обеспечения, отмечает, что «отсутствие четких критериев оценки эффективности работы подразделений по противодействию киберпреступности» является одним из факторов, препятствующих профессиональному развитию сотрудников и привлечению квалифицированных специалистов. Он предлагает, чтобы «выявление таких преступлений поощрялось, даже если виновные лица не установлены», а «к дополнительным преференциям должны приводить своевременное выявление и фиксация улик, получение оперативно значимой информации».

Отдельного рассмотрения заслуживает проблема использования систем искусственного интеллекта в деятельности правоохранительных органов. Если изначально использование таких систем (как «Криминалист», «Спрут» и др.) носило экспериментальный характер, то к 2025 году остро встал вопрос об их правовом статусе. Эксперты прямо указывают на правовой барьер: данные, полученные с помощью ИИ, не могут служить прямым доказательством в суде без изменений в УПК РФ. Таким образом, де-факто сложившаяся инновационная практика требует легитимации через де-юре уточнение процессуальных норм.

Как отмечается в научной литературе, «несмотря на бесспорные плюсы применения новых технологий в экспертной деятельности, авторами предлагается закрепить в УПК РФ принципы такого использования, что обусловлено назначением уголовного судопроизводства и его основополагающими принципами». Вместе с тем, практика применения ИИ уже существует: в Следственном комитете с его помощью выявляют закономерности преступного поведения, работает программа распознавания лиц, сопоставляющая изображения разыскиваемых с видеозаписями. В четырех регионах РФ нейросети переводят устную речь в текст при составлении протоколов заседаний. В Генеральной прокуратуре нейросети используют для обработки миллионов обращений граждан, криминологического прогноза и выявления долгосрочных рисков.

Вместе с тем, использование общедоступных ИИ-сервисов (вроде ChatGPT) при подготовке процессуальных документов создает серьезные процессуальные риски. Как отмечают специалисты, «использование общедоступных сервисов при подготовке протоколов нарушает требования ст. 161 УПК РФ о неразглашении данных предварительного расследования». Это создает риск нарушения тайны следствия при передаче данных в облачные сервисы и подмены «внутреннего убеждения» должностного лица алгоритмом.

Президент РФ поручил правительству, Верховному суду, МВД, Следственному комитету и ФСБ изучить целесообразность признания использования ИИ при совершении правонарушений отягчающим обстоятельством. Это поручение свидетельствует о признании необходимости правового регулирования данной сферы на высшем уровне.

Профессор Комлев, рассматривая перспективы цифрового социального контроля, подчеркивает, что он должен опираться на системное понимание природы кибердевиантности и учитывать контекстуальность социальных норм в цифровой среде. Интегративный подход, обоснованный в работах профессора Комлева, позволяет «при изучении кибердевиантности использовать методологическую триангуляцию, включающую методы бесконтактных опросов, фокус-группы, дискурсивный анализ, контент-анализ цифровой текстовой и видеоинформации, вычислительные алгоритмы для обработки структурированных и неструктурированных больших данных».

На основании выявленных тенденций и с учетом мнений исследователей можно предложить следующие направления для совершенствования законодательства, направленные на усиление защиты жертв киберпреступлений.

Необходимо дополнить УПК РФ специальной главой или статьями, регламентирующими: право на оперативную информационную и психологическую помощь – создание механизма немедленного подключения психологической службы и специалиста по цифровой безопасности при первичном обращении жертвы (особенно в случаях кибергруминга или травли); упрощенную процедуру обеспечения гражданского иска в киберпреступлениях, а также введение

возможности наложения обеспечительных мер (арест криптокошельков, электронных счетов) по заявлению потерпевшего на ранней стадии расследования на основе представленных им данных (скриншоты, логи переводов); гарантии защиты от ревиктимизации путем введения четких правил ограничения доступа обвиняемого и его защиты к персональным данным и цифровому контенту жертвы в ходе следствия.

П.С. Швыряев в своем исследовании подчеркивает, что «эффективная стратегия противодействия киберпреступности должна быть направлена на создание такого состояния системы, в котором вероятность эксплуатации уязвимостей минимизирована, а порог проникновения сквозь защитный барьер системы высок и сложен». Это предполагает не только технические меры, но и правовую защиту жертв на всех этапах уголовного судопроизводства.

На основе разработки и законодательного закрепления плана «Национального стандарта цифровой гигиены и реагирования на инциденты» 2025 года предлагается принять федеральный закон, обязывающий все организации, работающие с персональными данными (банки, соцсети, госорганы), внедрять единый модуль экстренного реагирования. Этот модуль должен предоставлять пользователю, заподозрившему мошенничество или ставшему жертвой атаки, чеклист действий (заблокировать карту, сменить пароли, сохранить доказательства) с возможностью автоматической отправки заявления в правоохранительные органы. В стандарт следует включить обязательные регулярные проверки цифровых следов для уязвимых категорий (дети, пожилые) с согласия их законных представителей с использованием этичных ИИ-алгоритмов, настроенных на выявление признаков груминга, буллинга или финансовых манипуляций.

Для преодоления дефицита экспертных ресурсов необходимо законодательно урегулировать порядок привлечения специалистов частных IT- и кибербезопасностных компаний к проведению экспертиз и оперативному анализу данных в рамках следственных действий на основе специального сертификата и в условиях соблюдения процессуальной тайны. Закон должен предусматривать механизм ответственности и страхования для таких частных экспертов, а также

иммунитет от претензий за добросовестное нарушение лицензионных соглашений (EULA) при исследовании вредоносного ПО в интересах следствия.

П.А. Скобликов подчеркивает, что «современная уголовная политика поощряет правоохранительные органы представлять искаженную, но приемлемую картину криминологической ситуации, а не противостоять неблагоприятным реалиям». Преодоление этого дисбаланса требует разработки и внедрения объективных критериев оценки эффективности, закрепленных на концептуальном уровне и последовательно реализуемых на практике.

В развитие предыдущих предложений представляется целесообразным сформулировать конкретные законопроекты и проект поправок в Уголовно-процессуальный кодекс РФ (в части использования технологий искусственного интеллекта).

1.Федеральный закон «О базовых гарантиях прав жертв киберпреступлений». Статья 1 устанавливает дополнительные гарантии правовой, социальной и психологической защиты лиц, пострадавших от преступлений, совершенных с использованием информационно-телекоммуникационных технологий. Статья 3 закрепляет право на экстренную цифровую помощь: каждый потерпевший вправе получить в течение 24 часов с момента обращения в правоохранительные органы консультацию специалиста по цифровой безопасности, направленную на минимизацию ущерба (блокировка учетных записей, отзыв компрометированных данных, настройка защиты). Финансирование обеспечивается за счет средств фонда, формируемого из конфискованных у киберпреступников активов. Статья 5 предусматривает создание обезличенного государственного реестра моделей, схем и цифровых следов кибератак для анализа и профилактики. Банки, операторы связи и иные организации обязаны вносить в него данные об инцидентах. Потерпевшие вправе бесплатно получить справку о внесении своего случая в реестр для обращения в суд или страховую компанию.

2. Проект поправок в Уголовно-процессуальный кодекс РФ (в части использования технологий искусственного интеллекта). Предлагается ввести новую статью 164.1 «Особенности проведения следственных действий с

использованием систем искусственного интеллекта». Пункт 1 устанавливает допустимость данных, полученных в результате обработки информации системами искусственного интеллекта, сертифицированными уполномоченным Правительством РФ органом, в качестве источника доказательств. Пункт 2 требует процессуального оформления результатов работы системы ИИ в виде заключения специалиста, в котором в обязательном порядке раскрываются использованные алгоритмы, набор данных для обучения и степень вероятности вывода. Алгоритм не может быть засекречен от защиты и суда. Пункт 3 вводит этические ограничения: запрещается использование систем ИИ, осуществляющих оценку личности, прогнозирование потенциальной преступной деятельности лица, не причастного к расследуемому событию, а также массовый нецелевой скрининг личных коммуникаций.

Правовая инновация в сфере противодействия киберпреступности в России к 2025 году действительно представляет собой яркий пример позитивной девиации. Система последовательно отклоняется от архаичных, неэффективных в цифровую эпоху подходов: от узкого имущественного понимания вреда к комплексной защите личности, от политизированных международных схем к технологичному доказательному сотрудничеству, от пассивного ожидания обращений граждан к активной превенции с использованием ИИ.

Как показывает анализ научной литературы, проведенный 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. Профессор Комлев обоснованно утверждает, что подготовку киберполицейских «предлагается реализовать в ведомственной образовательной системе, где сформирован фундамент правовых, девиантологических исследований и знаний с привлечением специалистов из IT-сферы и правоприменительной практики». При этом он подчеркивает необходимость интегративного подхода к

изучению кибердевиантности, что имеет прямое отношение к формированию образовательных стандартов для киберполицейских.

А.Ю. Сергеев и О.В. Широкова акцентируют внимание на том, что мошенничество в цифровом обществе «приобретает системный характер, а его профилактика требует не только правовых, но и социально-психологических мер воздействия на потенциальных жертв и преступников». Этот вывод согласуется с предложениями о формализации прав жертв и внедрении стандартов цифровой гигиены.

П.С. Швыряев обосновывает, что «эффективная стратегия противодействия киберпреступности может быть выстроена на основе концепции устойчивого цифрового развития», которая предполагает «такой подход к проектированию, внедрению и масштабированию цифровых продуктов и устройств, который обеспечивает минимальные риски зарождения и распространения преступной деятельности». Стратегия должна базироваться на принципах «системности, долговременности, непрерывности

Список литературы

1. Комлев Ю.Ю. Девиантное поведение и нормообразование: от протоморали к контекстуально выстроенному сконструированному праву эпохи постмодерна и интегративному изучению преступности / Ю.Ю. Комлев. – URL: https://cyberleninka.ru/article/n/deviantnoe-povedenie-i-normoobrazovanie-ot-protomorali-k-kontekstualno-vystroennomu-skonstruirovannomu-pravu-epohi-postmoderna-i (дата обращения: 18.06.2026).

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

3. Сергеев А.Ю. Мошенничество в цифровом обществе: социально-правовой анализ / А.Ю. Сергеев, О.В. Широкова // Вопросы криминологии. – 2025. – №3. – С. 45–58.

4. Швыряев П.С. Киберпреступность как социально-технический феномен : дис. ... канд. социол. наук / П.С. Швыряев. – М.: МГУ имени М.В. Ломоносова, 2025. – 189 с.

5. Фомин Е.В. К вопросу о понятийном аппарате киберпреступности / Е.В. Фомин // Правовая информатика. – 2024. – №5. – С. 33–41.

6. Костенко Р.В. Проблемы нормативного обеспечения прозрачности экспертной деятельности при использовании новых технологий для анализа доказательств (на примере машинного обучения) / Р.В. Костенко, М.А. Духанова // Закон и право. – 2025. – №5. – С. 210–214. DOI 10.24412/2073-3313-2025-5-210-214. EDN ULBBHD

7. Конвенция ООН против киберпреступности (Ханойская конвенция): принята Генеральной Ассамблеей ООН в декабре 2024 г., подписана Российской Федерацией 25 октября 2025 г. // Официальный сайт ООН. – URL: https://www.un.org/cybercrime-convention (дата обращения: 18.06.2026).

8. Конвенция Совета Европы о преступности в сфере компьютерной информации (Будапештская конвенция): заключена в г. Будапеште 23 ноября 2001 г. // Собрание законодательства РФ. – 2009. – №12. – Ст. 1308.

9. Концепция государственной системы противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий: утв. распоряжением Правительства РФ от 30 декабря 2024 г. №4154-р // Собрание законодательства РФ. – 2025. – №2. – Ст. 215.

10. Об утверждении плана мероприятий по реализации Концепции государственной системы противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий: распоряжение Правительства РФ от 14 августа 2025 г. №2207-р // Собрание законодательства РФ. – 2025. – №34. – Ст. 4120.

11. Уголовный кодекс Российской Федерации: Федеральный закон от 13 июня 1996 г. №63-ФЗ (ред. от 28.04.2026) // Собрание законодательства РФ. – 1996. – №25. – Ст. 2954.

12. Уголовно-процессуальный кодекс Российской Федерации: Федеральный закон от 18 декабря 2001 г. №174-ФЗ (ред. от 30.03.2026) // Собрание законодательства РФ. – 2001. – №52 (ч. I). – Ст. 4921.

13. Генпрокурор Гуцан подписал в Ханое Конвенцию ООН против киберпреступности // Российская газета. – 2025. – 25 октября. – URL: https://rg.ru/amp/2025/10/25/genprokuror-gucan-podpisal-v-hanoe-konvenciiu-oon-protiv-kiberprestupnosti.html (дата обращения: 18.06.2026).

14. Правительство утвердило Концепцию государственной системы противодействия преступлениям, совершаемым с помощью информационно-коммуникационных технологий // Официальный сайт Правительства Российской Федерации. – 2025. – 9 января. – URL: http://government.ru/dep_news/53922/ (дата обращения: 18.06.2026).

15. Судьба Конвенции ООН о противодействии киберпреступности: будет ли поддержана российская инициатива? // Совет по развитию гражданского общества и правам человека. – 2024. – 8 февраля. – URL: http://www.president-sovet.ru/members/blogs/post/sudba_konventsii_oon_o_protivodeystvii_kiberprestupnosti_budet_li_podderzhana_rossiyskaya_initsiativ/ (дата обращения: 18.06.2026).

16. Использование ИИ-сервисов при подготовке протоколов нарушает требования статьи 161 УПК // Уголовный процесс. – 2026. – 30 апреля. – URL: https://www.ugpr.ru/news/9808-ispolzovanie-ii-servisov-pri-podgotovke-protokolov-narushaet-trebovaniya-stati-161-upk (дата обращения: 18.06.2026).

17. Церемония подписания Конвенции ООН против киберпреступности открывается сегодня в Ханое // Иллюстрированный журнал Вьетнам на русском языке. – 2025. – 24 октября. – URL: https://vietnam.vnanet.vn/russian/ (дата обращения: 22.06.2026).

18. CoE at the Signing Ceremony of the UN Convention against Cybercrime in Hanoi // UNODC-KOSTAT Centre of Excellence. – 2025. – 25–27 October. – URL: https://coekostat.unodc.org/coekostat/en/news/20251025–27_coe-at-the-signing-ceremony-of-the-un-convention-against-cybercrime-in-hanoi.html (дата обращения: 18.06.2026).