ТРАНСФОРМАЦИЯ ПРЕСТУПНОСТИ В ЦИФРОВОЙ СРЕДЕ

Струков В.Н.[1]

Ключевые слова: *цифровая среда, киберпреступность, неправомерный доступ, цифровая грамотность, подростковая вовлеченность, сетевые платформы, правовое регулирование, профилактика преступлений, виктимизация.*

Аннотация

Цель работы *состоит в анализе влияния цифровизации общественных отношений на трансформацию преступной деятельности и разработке подходов к противодействию новым формам противоправных практик в виртуальной среде.*

Метод исследования *основан на комплексном применении общенаучных и частнонаучных методов. Использованы методы анализа и синтеза для выявления ключевых тенденций развития преступности в условиях цифровизации. Проведен сравнительно-правовой анализ действующего законодательства и правоприменительной практики. Применен формально-юридический метод для интерпретации норм уголовного права, а также элементы криминологического подхода при исследовании виктимологических аспектов и факторов вовлечения различных социальных групп в противоправную деятельность.*

Результаты исследования *показали, что развитие цифровых технологий приводит к качественной трансформации преступности, формируя новые формы противоправного поведения, характеризующиеся дистанционностью, анонимностью и высокой степенью латентности. Установлено, что неправомерный доступ к цифровым ресурсам все чаще выступает не как самостоятельное деяние, а как начальный этап более сложных преступных схем, включая хищения и незаконные операции. Выявлена тенденция формирования «комбинированных» преступлений, при которых одно деяние служит технологической основой для другого, усиливая общественную опасность. Определено, что наибольшей уязвимостью обладают несовершеннолетние и лица старшего возраста, что обусловлено либо недостаточной правовой осведомленностью, либо доверием к цифровым источникам. Сделан вывод о необходимости совершенствования нормативной базы, повышения уровня цифровой грамотности населения и развития специализированных компетенций правоохранительных органов. В работе представлены теоретические модели вовлечения несовершеннолетних в противоправные действия в цифровой среде, а также конкретные законодательные, технические и организационные меры противодействия таким явлениям. Реализация предложенных подходов к противодействию новым формам противоправных практик в виртуальной среде позволит снизить виктимизацию уязвимых групп населения и повысить эффективность профилактики.*

DOI: 10.24412/1994-1404-2026-2-273-279

Введение

В настоящее время развитие информационно-коммуникационных технологий не стоит на месте. Они выступают катализатором улучшения жизнедеятельности граждан, но одновременно становятся источником новых криминальных практик и стимулируют трансформацию преступной деятельности. Рост преступлений, совершаемых с использованием информационно-коммуникационных технологий, подтверждается официальными данными правоохранительных органов[2] (табл. 1).

[2] Состояние преступности // Официальный сайт МВД России. URL: https://мвд.рф (дата обращения: 20.02.2026).

[1] ***Струков Виктор Николаевич****, кандидат юридических наук, доцент кафедры криминалистики Белгородского юридического института МВД России им. И.Д. Путилина, г. Белгород, Россия.*

E-mail: str-v-n@yandex.ru

Таблица 1

Динамика преступлений в сфере ИКТ в Российской Федерации

Год	Общее количество IT-преступлений
2022	522 065
2023	676 951
2024	765 400

Так, по данным МВД России, в 2024 году зарегистрировано 765,4 тыс. преступлений в сфере информационно-коммуникационных технологий, что на 13,1% больше по сравнению с предыдущим годом.

В последнее время все чаще преобладает дистанционный характер совершения преступлений, который осуществляется с помощью широкого спектра цифровых устройств — от смартфонов до персональных компьютеров. Данный технологический процесс не только порождает новые формы криминальных посягательств, но и предоставляет злоумышленникам инструменты для сокрытия следов преступлений.

Особое опасение вызывает рост киберпреступности в цифровой среде, затрагивающий в том числе уязвимые социальные группы — в частности, подростков, активно вовлеченных в использование сетевых платформ. Подростковая вовлеченность в цифровые сервисы повышает риски их виктимизации. Недостаточная цифровая грамотность делает несовершеннолетних легкой мишенью для манипуляций и противоправных действий — от фишинга[3] до вовлечения в преступные схемы [1].

Как следствие, перед правоохранительными органами обостряется проблема эффективного раскрытия и расследования таких преступлений, выраженная дефицитом специальных компетенций и необходимостью постоянного наращивания экспертного потенциала в цифровой сфере [2, 3]. Существующие методы работы зачастую не успевают за темпами трансформации преступной деятельности: злоумышленники оперативно адаптируют тактики под новые технологии, используют анонимные сети и криптографические инструменты, усложняя идентификацию и сбор доказательств.

Расширение спектра противоправных действий — от неправомерного доступа к цифровым ресурсам до сложных комбинированных схем, где одно преступление служит технологической основой для другого, — актуализирует необходимость совершенствования правового регулирования и усиления профилактики преступлений. В этих условиях критически важно повышать уровень цифровой грамотности населения, особенно среди несовершеннолетних, а также разрабатывать комплексные меры по снижению виктимизации пользователей в виртуальной среде.

Постановка задач

Правовой вызов, порождаемый цифровым разрывом в компетенциях, усугубляется именно тем, что несовершеннолетние показывают самый высокий уровень вовлеченности в цифровую сферу, которые, в силу возрастных особенностей, являются наиболее уязвимой категорией пользователей. Легкость освоения цифровых интерфейсов приводит к тому, что дети и подростки, активно познающие мир через веб-сайты, приложения и мессенджеры, зачастую не осознают связанных с этим правовых и криминальных рисков.

Несовершеннолетние могут стать невиновными жертвами мошеннических схем (например, осуществив несанкционированный платеж с банковской карты законного представителя под предлогом приобретения цифрового контента), что в дальнейшем создает серьезную угрозу, быть вовлеченными в преступную деятельность [4].

Целью настоящего исследования является оценка влияния цифровизации общественных отношений на трансформацию преступной деятельности, выявление особенностей вовлечения несовершеннолетних — наиболее уязвимой категории пользователей — в противоправные схемы, а также раскрытие правовых и криминологических аспектов современных форм преступности, включая механизмы виктимизации подростков в цифровой среде.

Для достижения указанной цели в работе решаются следующие задачи:

1. Выявить структурные изменения преступности под влиянием цифровизации, включая феномен киберпреступных каскадов (неправомерный доступ как основа для последующих тяжких преступлений), путем анализа динамики и структуры преступности в условиях цифровизации за последние 3 года на основе официальной статистики МВД РФ, а также выделения ключевых видов киберпреступлений, формирующих «каскадные» схемы, — в том числе неправомерного доступа к компьютерной информации, фишинга, мошенничества с платежными данными, распространения вредоносного программного обеспечения и атак на корпоративные сети.
2. Определить социально-правовые особенности вовлечения несовершеннолетних в цифровую преступность посредством выявления основных каналов и механизмов вовлечения подростков в противоправные действия в цифровой среде.
3. Сформулировать конкретные предложения по совершенствованию законодательства, профилактике и повышению компетенций правоохранительных органов.

[3] Фишинг (от англ. phishing, производного от fishing — «рыбная ловля, выуживание») — это вид киберпреступления или интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей: логинам, паролям, номерам банковских карт, личным данным и другой чувствительной информации.

Последовательное решение поставленных задач создает необходимую научную и практическую базу для реализации целей исследования и выработки мер, направленных на снижение уровня киберпреступности и защиту уязвимых групп населения в цифровой среде.

Решение поставленных задач

Цифровизация как фактор трансформации преступности

Эволюция IT-сферы как детерминанта роста преступности основывается на формировании сложно интегрированной цифровой среды, что порождает качественно новые криминогенные риски. Ключевая особенность заключается в инструментально-средовом дуализме информационных технологий: одно противоправное деяние может выступать не только как самостоятельное преступление, но и как технологическая база для совершения последующих, более тяжких преступлений, образуя так называемые киберпреступные каскады.

Иллюстрацией данной модели служит неправомерный доступ к компьютерной информации. В современных условиях данный состав редко выступает как самоцель, трансформируясь в ключевую стадию реализации комплексных криминальных схем. Незаконно полученный доступ к учетным записям предоставляет злоумышленникам возможность не только хищения конфиденциальных данных, но и использования этих ресурсов в дальнейшей преступной деятельности [5].

Механизмы формирования киберпреступных каскадов

Эксплуатация скомпрометированных аккаунтов осуществляется по двум основным направлениям:

1. В сфере незаконного оборота наркотических средств — использование аккаунтов как канала коммуникации для координации действий и распространения информации о «закладках», что затрудняет идентификацию истинного субъекта преступления [6].
2. В целях совершения мошенничества — применение методов социальной инженерии, при которых от имени владельца аккаунта рассылаются сообщения с просьбами о финансовой помощи, что значительно повышает уровень доверия и эффективность преступления [7].

Отдельный сегмент криминального использования связан с цифровыми платформами (например, маркетплейсами). Завладение учетными записями позволяет манипулировать репутационными показателями товаров, формируя фиктивные отзывы и вводя потребителей в заблуждение.

Киберкаскады качественно повышают общественную опасность, поскольку одно деяние становится технологической основой для мошенничества или наркоторговли. При этом для реализации каскадных схем организаторам требуются «технические исполнители» — роль, которую в силу возрастных и психологических особенностей часто выполняют несовершеннолетние.

Особенности вовлечения несовершеннолетних в цифровую преступность

Путем эксплуатации правовой наивности и экономических интересов несовершеннолетних злоумышленники предлагают им «легкий заработок» в качестве, например, «закладчика» наркотических средств или участника иных противоправных действий в сети. Ключевым элементом подобных манипуляций является формирование у подростка ложного чувства безнаказанности, основанного на неверном толковании возраста уголовной ответственности.

По ряду составов преступлений, совершаемых с использованием информационно-коммуникационных технологий, применяются следующие нормы Уголовного кодекса Российской Федерации от 13 июня 1996 г. № 63-ФЗ (далее — УК РФ):

1. Ст. 228.1 — незаконный оборот наркотических средств с использованием средств массовой информации либо информационно-телекоммуникационных сетей, включая сеть «Интернет»;
2. Ст. 159.3 — мошенничество с использованием электронных средств платежа;
3. Ст. 159.6 — мошенничество в сфере компьютерной информации;
4. Ст. 272 — неправомерный доступ к компьютерной информации[4].

Следует отметить, что уголовная ответственность по общему правилу наступает с 16 лет (ч. 1 ст. 20 УК РФ), однако за ряд преступлений — с 14 лет (ч. 2 ст. 20 УК РФ). В рамках рассматриваемых составов применяется преимущественно общий возрастной порог. Рассматриваемые составы преступлений, как правило, предусматривают наступление уголовной ответственности с 16 лет. При этом отсутствие уголовной ответственности в ряде случаев не означает полной безнаказанности несовершеннолетних, поскольку их действия могут влечь административную ответственность, постановку на профилактический учет и применение мер воспитательного воздействия.

В рамках исследования выявлены следующие особенности вовлечения несовершеннолетних в преступную деятельность с использованием информационно–коммуникационных технологий (ИКТ):

1. Эксплуатация правовой наивности и недостаточной осведомленности об уголовной ответственности;

[4] Уголовный кодекс Российской Федерации: федеральный закон от 13 июня 1996 г. № 63-ФЗ (ред. от 15.10.2025) // Собрание законодательства РФ. 1996. № 25. Ст. 2954.

2. Ложное представление о безнаказанности, связанное с общим возрастом наступления ответственности (16 лет) по большинству составов;
3. Низкий порог входа в противоправную схему (регистрация аккаунта, перевод денег, передача посылки);
4. Отсутствие у несовершеннолетних критического восприятия анонимных цифровых коммуникаций и инструкций от «кураторов».

Таким образом, анализ выявленных особенностей позволяет выделить ключевые причины выбора несовершеннолетних в качестве участников преступных схем. Это: низкий уровень правовой осведомлённости; повышенная восприимчивость к манипулятивным техникам; мотивация, связанная со стремлением к быстрому получению материального вознаграждения; ошибочное представление о собственной безнаказанности ввиду возрастных ограничений уголовной ответственности.

Теоретические модели вовлечения несовершеннолетних

Опираясь на выявленные особенности вовлечения несовершеннолетних в преступную деятельность с использованием информационно-коммуникационных технологий, в рамках исследования сформулированы две теоретические модели такого вовлечения.

1. Модель «инструментального исполнителя» — подросток выступает техническим агентом (дроппер[5], рассылка фишинговых сообщений, перевод денег), не осознавая конечной цели и механизма всего преступного каскада. Снижение риска для организатора достигает 80—90%, поскольку несовершеннолетний не обладает полной информацией о заказчике.
2. Модель «псевдоработодателя» — через Telegram-каналы, группы в соцсетях и мессенджеры несовершеннолетнему обещается легкий доход за простые действия (проголосовать, перевести небольшую сумму, получить и переслать посылку, установить приложение). У подростка формируется ложный локус контроля: он убежден, что «ничего преступного не делает», поскольку действует по инструкции и за небольшие деньги.

Указанные особенности активно используются организаторами преступных схем для минимизации собственных рисков, что делает модель вовлечения несовершеннолетних стратегически выгодной. По данным правоохранительных органов, в последние годы наблюдается рост вовлечения несовершеннолетних в такие преступные схемы, как дропперство, интернет-мошенничество и распространение наркотических средств через систему «закладок»[6].

Цифровая среда, обладая такими характеристиками, как доступность, анонимность и высокая скорость взаимодействия, одновременно формирует благоприятные условия для развития преступной деятельности. По мнению Кулаевского А.В., низкая раскрываемость дистанционных преступлений обусловлена отсутствием у правоохранительных органов необходимого технического обеспечения и недостаточной компетентностью сотрудников в сфере киберпреступности [8].

Таким образом, вовлечение несовершеннолетних представляет собой не случайное явление, а устойчивую криминальную практику, обусловленную как социально-психологическими, так и правовыми факторами.

Статистика вовлечения несовершеннолетних: динамика и масштабы проблемы

Динамика вовлечения несовершеннолетних в IT-преступления представлена в табл. 2.

Таблица 2

Вовлечение несовершеннолетних в IT-преступления

Год	Преступления с участием несовершеннолетних	Доля от IT-преступлений
2022	47,3 тыс.	7,6%
2023	56,9 тыс.	8,4%
2024	68,0 тыс.	8,9%

Как следует из табл. 2, в 2024 году из 765,4 тыс. преступлений, совершенных с использованием информационно-коммуникационных технологий, около 68 тыс. (8,9%) были связаны с деятельностью несовершеннолетних. Это подтверждается динамикой предыдущих лет: в 2022 году таких преступлений было 47,3 тыс. (7,6%), а в 2023 г. — 56,9 тыс. (8,4%), что указывает на устойчивый рост вовлечения подростков в цифровую преступность[7].

Помимо этого, более 40 % всех зарегистрированных преступлений, совершенных с использованием цифровых технологий, составляли мошеннические схемы, а около 22 % — преступления, связанные с не-

[5] Дроппер (от англ. drop — «сбрасывать, перекидывать») — физическое лицо, которое выступает промежуточным звеном в схемах незаконного оборота денежных средств: предоставляет преступникам доступ к своим банковским счетам, картам или электронным кошелькам либо выполняет по их указанию финансовые операции.

[6] По данным Альянса по защите детей в цифровой среде, в 2025 году в 74 раза возросло втягивание детей в совершение киберпреступлений относительно 2023 года. Среди таких преступлений упоминаются дропперство, установка вредоносного ПО, поджоги и другие. При этом около 37% из 1,8 млн россиян, которым грозят уголовные сроки за дропперство, — несовершеннолетние // Российская газета. 2025. 23 сентября. URL: https://rg.ru/2025/09/23 (дата обращения 29.04.2026).

[7] Состояние преступности // Официальный сайт МВД России. URL: https://мвд.рф (дата обращения: 20.02.2026).

законным оборотом наркотических средств через цифровые каналы связи.

Таким образом, проблема вовлечения подростков в цифровую преступность не только приобретает масштабный характер, но и затрагивает наиболее социально опасные виды противоправных действий, что требует незамедлительного внедрения комплексных профилактических и правоприменительных мер [9—10].

Предложения по противодействию киберпреступным каскадам и вовлечению уязвимых групп населения в преступную деятельность

Для снижения уровня вовлечения подростков в противоправные действия в цифровой среде предлагается:

1. Ввести в школах (5—9 классы) обязательный модуль «Цифровая кибербезопасность» (объёмом не менее 8 часов в год) с практическими примерами о дропперстве[8], фишинге, ответственности за неправомерный доступ и вовлечение в наркоторговлю.
2. В рамках внеурочной деятельности организовать просветительские мероприятия и тестирование для родителей по вопросам цифровой безопасности и признаков вовлечения детей в преступные схемы.
3. Разработать и запустить на популярных цифровых платформах (соцсети, мессенджеры, игровые сервисы) информационные кампании с разъяснением рисков участия в сомнительных схемах («закладки», дропперство, фейковые опросы и т.д.).
4. Создать на базе образовательных организаций и центров молодёжного развития программы наставничества, где старшеклассники и студенты под руководством психологов и юристов будут обучать младших сверстников основам цифровой гигиены и правовой грамотности.
5. Обеспечить доступ к анонимной онлайн консультации с юристами и психологами для несовершеннолетних, столкнувшихся с предложениями «лёгкого заработка» в сети.

Для борьбы с цепочками взаимосвязанных киберпреступлений предлагается:

1. Внести изменения в ст. 272 УК РФ («Неправомерный доступ к компьютерной информации»), дополнив часть 2 пунктом «г»: «то же деяние, совершённое с целью последующего совершения тяжкого или особо тяжкого преступления» — с санкцией в виде лишения свободы на срок от 5 до 8 лет. Это позволит квалифицировать киберкаскады как единый преступный умысел.
2. Создать в каждом федеральном округе специализированный отдел по расследованию «киберкаскадных» преступлений. В штат включить следователей с обязательной сертификацией по направлению «Информационная безопасность и расследование киберпреступлений» (на базе ведомственных вузов). Установить для них повышенный коэффициент сложности (стимулирующую выплату).
3. Наладить межведомственное взаимодействие между МВД, ФСБ, Роскомнадзором и банками для оперативного обмена данными о подозрительных транзакциях и скомпрометированных учетных записях.

Для комплексной защиты пожилых людей и иных уязвимых категорий граждан целесообразно принять следующие меры:

1. Обязать операторов сотовой связи бесплатно подключать антифишинговый сервис для абонентов старше 65 лет. Сервис должен автоматически блокировать SMS-сообщения с подозрительными ссылками, фильтровать фишинговые сообщения и предупреждать пользователя о потенциально опасных сообщениях с разъяснением причин такого предупреждения.
2. Организовать бесплатные курсы цифровой грамотности в центрах социального обслуживания, библиотеках и других доступных местах. Программы курсов должны включать практические занятия по распознаванию фишинга, работе с мобильными приложениями и защите личных данных — это поможет повысить общую осведомлённость и снизить риск стать жертвой мошенников.

Реализация предложенных мер потребует тесной координации между государственными органами, бизнесом и образовательными учреждениями, а также регулярного обновления систем с учётом появления новых угроз. Комплексный подход позволит существенно снизить уровень виктимности уязвимых групп населения, повысить их цифровую грамотность и обеспечить оперативную защиту от актуальных киберугроз.

Выводы

Эволюция информационно-коммуникационных технологий носит амбивалентный характер: с одной стороны, она способствует прогрессу, с другой — создает благоприятную среду для дистанционных преступлений и вовлечения несовершеннолетних. Генпрокуратура РФ фиксирует устойчивый рост использования подростков в качестве дропперов, распространителей фишинга и вредоносных программ, что подтверждает необходимость усиления профилактических мер.

[8] Дропперство (от англ. dropper — «тот, кто бросает/передаёт») — противоправная деятельность, при которой физическое лицо (дроппер) используется как промежуточное звено в схемах незаконного оборота денежных средств.

Научная новизна исследования заключается в трех результатах. Во-первых, выявлен и описан феномен «киберпреступных каскадов» — модели, при которой неправомерный доступ (ст. 272 УК РФ) выступает технологической основой для последующих тяжких преступлений (мошенничество, наркоторговля). Во-вторых, разработаны две теоретические модели вовлечения несовершеннолетних: «инструментальный исполнитель» (подросток как технический агент, не осознающий конечной цели) и «псевдоработодатель» (формирование ложного локуса контроля через обещание легкого дохода). В-третьих, сформулирован комплекс конкретных мер противодействия.

Практическая значимость работы подтверждается механизмами реализации предложений. Для решения выявленных проблем предлагается три шага. На законодательном уровне — дополнить ст. 272 УК РФ квалифицирующим признаком «неправомерный доступ с целью последующего совершения тяжкого преступления». В рамках просветительской деятельности целесообразно внедрить в школьную программу обязательный модуль «Основы цифровой безопасности», включающий анализ практических ситуаций, иллюстрирующих схемы вовлечения граждан в незаконный оборот денежных средств и методы хищения персональных данных посредством обмана. В организационно-технической плоскости — создать в каждом федеральном округе специализированные отделы по расследованию киберкаскадных преступлений с сертификацией следователей. Реализация указанных мер позволит квалифицировать киберкаскады как единый преступный умысел, снизить вовлечение несовершеннолетних и повысить раскрываемость.

Таким образом, цифровая трансформация преступности носит не количественный, а качественный характер. Предложенные теоретические модели и практические шаги создают основу для системного противодействия вовлечению несовершеннолетних в цифровую преступность.

Литература

1. Кафарова Р.Д. Вовлечение несовершеннолетних в преступления в сфере информационно-телекоммуникационных технологий в современной России // Мониторинг правоприменения. 2025. № 3 (56). С. 90—95.
2. Кувшинова В.С. Криминологическая характеристика киберпреступности // Международный журнал гуманитарных и естественных наук. 2020. № 5-4. С. 53—57.
3. Андрюшенков В.А., Андрюшенкова О.М. Использование информационных технологий как способ совершения преступлений // Закон и право. 2024. № 5. С. 208—213.
4. Хохлова А.Ю. Проблемы противодействия незаконному обороту наркотических средств с использованием сети Интернет // Конституции России 30 лет. 2024. С. 182—185.
5. Морозов Д.А. Преступления в сфере компьютерной информации: проблемы квалификации // Уголовное право. 2022. № 4. С. 67—72.
6. Третьяков Г.М. Информационные технологии в структуре способа совершения преступлений, связанных с незаконным оборотом наркотических средств // Вестник Гродненского государственного университета имени Янки Купалы. Серия 4. Правоведение. 2021. Т. 11. № 1. С. 96—103.
7. Сидоров А.К. Виктимологические аспекты цифровой преступности // Журнал российского права. 2021. № 9. С. 98—104.
8. Кулаевский А.В., Козлов Д.Ю., Юрьев М.А. Разработка системы поддержки принятия решений, действий следователя при расследовании дистанционного мошенничества // Правовая информатика. 2025. № 4. С. 119—126.
9. Власова Е.В. Незаконный оборот наркотических средств с использованием сети Интернет // Юридический факт. 2019. № 47. С. 40—42.
10. Носова Д.Х., Муханов Ю.В., Цуров Т.Б. Формирование готовности сотрудников полиции к профилактике преступности несовершеннолетних в сети Интернет // Human Progress. 2025. Т. 11. № 10.

SECTION:
CONSTITUTIONAL LAW

TRANSFORMATION OF CRIME IN THE DIGITAL ENVIRONMENT

Strukov V.N.[9]

Keywords: *digital environment, cybercrime, unauthorized access, digital literacy, adolescent engagement, online platforms, legal regulation, crime prevention, victimization.*

Abstract

Purpose of work *is to analyse the impact of digitalization of social relations on the transformation of criminal activity and to develop approaches to countering emerging forms of unlawful practices in the virtual environment.*

The research methodology *is based on the integrated application of general scientific and specific scientific methods. Analytical and synthetic methods were employed to identify key trends in the development of crime under conditions of digitalization. A comparative legal analysis was conducted of current legislation and law enforcement practice. The formal-legal method was applied to interpret criminal law norms, complemented by elements of a criminological approach in examining victimological aspects and factors contributing to the involvement of various social groups in unlawful activities.*

Results of the study *demonstrate that the advancement of digital technologies leads to a qualitative transformation of crime, giving rise to new forms of unlawful conduct characterized by remote operation, anonymity, and a high degree of latency. It has been established that unauthorized access to digital resources increasingly functions not as an independent offence but as the initial stage of more complex criminal schemes, including theft and illicit financial operations. A trend towards the emergence of "combined" crimes has been identified, wherein one unlawful act serves as the technological foundation for subsequent offences, thereby amplifying overall societal risk. It has been determined that minors and elderly individuals are particularly vulnerable, due to either insufficient legal awareness (among adolescents) or excessive trust in digital sources (among older adults). The study concludes that there is a pressing need to improve the regulatory framework, enhance the population's digital literacy, and develop specialized competencies within law enforcement agencies. The paper presents theoretical models of adolescent involvement in unlawful actions within the digital environment, along with specific legislative, technical, and organizational countermeasures. Implementing the proposed approaches to countering new forms of unlawful practices in the virtual environment is expected to reduce the level of victimization among vulnerable population groups and enhance the effectiveness of crime prevention efforts in the context of digitalization.*

References

1. Kafarova R.D. Vovlechenie nesovershennoletnikh v prestupleniia v sfere informatsionno-telekommunikatsionnykh tekhnologii v sovremennoi Rossii // Monitoring pravoprimeneniia. 2025. No. 3 (56). S. 90—95.
2. Kuvshinova V.S. Kriminologicheskaia kharakteristika kiberprestupnosti // Mezhdunarodnyi zhurnal gumanitarnykh i estestvennykh nauk. 2020. No. 5-4. S. 53—57.
3. Andriushenkov V.A., Andriushenkova O.M. Ispol'zovanie informatsionnykh tekhnologii kak sposob sovershеniia prestuplenii // Zakon i pravo. 2024. No. 5. S. 208—213.
4. Khokhlova A.Iu. Problemy protivodeistviia nezakonnomu oborotu narkoticheskikh sredstv s ispol'zovaniem seti Internet // Konstitutsii Rossii 30 let. 2024. S. 182—185.
5. Morozov D.A. Prestupleniia v sfere komp'iuternoi informatsii: problemy kvalifikatsii // Ugolovnoe pravo. 2022. No. 4. S. 67—72.
6. Tret'iakov G.M. Informatsionnye tekhnologii v strukture sposoba sovershеniia prestuplenii, sviazannykh s nezakonnym oborotom narkoticheskikh sredstv // Vestnik Grodnenskogo gosudarstvennogo universiteta imeni Ianki Kupaly. Seriia 4. Pravovedenie. 2021. T. 11. No. 1. S. 96—103.
7. Sidorov A.K. Viktimologicheskie aspekty tsifrovoi prestupnosti // Zhurnal rossiiskogo prava. 2021. No. 9. S. 98—104.
8. Kulaevskii A.V., Kozlov D.Iu., Iur'ev M.A. Razrabotka sistemy podderzhki priniatiia reshenii, deistvii sledovatelia pri rassledovanii distantsionnogo moshennichestva // Pravovaia informatika. 2025. No. 4. S. 119—126.
9. Vlasova E.V. Nezakonnyi oborot narkoticheskikh sredstv s ispol'zovaniem seti Internet // Iuridicheskii fakt. 2019. No. 47. S. 40—42.
10. Nosova D.Kh., Mukhanov Iu.V., Tsurov T.B. Formirovanie gotovnosti sotrudnikov politsii k profilaktike prestupnosti nesovershennoletnikh v seti Internet // Human Progress. 2025. T. 11. No. 10.

[9] ***Viktor N. Strukov***, *Ph.D. (Law), Associate Professor of the Criminology Department, Belgorod Law Institute of the Ministry of Internal Affairs of Russia named after I.D. Putilin, Belgorod, Russia.*
E-mail: str-v-n@yandex.ru