Дата поступления рукописи в редакцию: 28.01.2026 г.
Дата принятия рукописи в печать: 10.03.2026 г.
DOI: 10.24412/2076-1503-2026-2-851-856

БАЖАНОВ Сергей Андреевич,
ведущий научный сотрудник отдела по совершенствованию нормативно-правового регулирования деятельности уголовно-исполнительной системы центра изучения проблем управления и организации исполнения наказаний в уголовно-исполнительной системе ФКУ НИИ ФСИН России,
e-mail: sergey.bazhanov62@yandex.ru

ЦИФРОВАЯ ТРАНСФОРМАЦИЯ ПРЕСТУПНОСТИ И ЭВОЛЮЦИЯ РОССИЙСКОЙ КРИМИНОЛОГИЧЕСКОЙ ПОЛИТИКИ: ВИКТИМОЛОГИЧЕСКИЕ И ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИЕ АСПЕКТЫ

Аннотация. *Цифровизация общественных отношений изменила не только инструменты коммуникации и экономического обмена, но и механизмы криминального поведения, что объективно требует пересмотра приоритетов российской криминологической политики. В статье исследуются ключевые направления влияния цифровых технологий на преступность: «гибридизация» криминальных практик, размывание границ между офлайн- и онлайн-средой, рост социальной инженерии как массового способа посягательств, усиление виктимологических рисков вследствие самораскрытия в цифровой среде, а также институционализация теневых рынков в анонимных сегментах сети. Показано, что цифровой след становится универсальным ресурсом раскрытия, доказывания и предупреждения преступлений, однако его использование связано с рисками утраты, модификации и фрагментации данных, что требует унификации процедур фиксации и обеспечения целостности. Обоснована перспективность использования распределённых реестров для учёта криминологически значимой информации и технологий больших данных/искусственного интеллекта для мониторинга и раннего выявления угроз при условии строгих правовых гарантий, аудита и ответственности. Особое внимание уделено кадровому обеспечению: цифровая преступность сочетает технические и социально-психологические механизмы, что обусловливает необходимость междисциплинарной подготовки специалистов и системной профилактики цифровой виктимизации населения. В выводах сформулированы практико-ориентированные положения о направлениях развития российской криминологической политики в условиях цифрового общества.*

Ключевые слова: *цифровая криминология; киберпреступность; криминологическая политика; цифровой след; социальная инженерия; даркнет; большие данные; искусственный интеллект; кибервиктимология.*

BAZHANOV Sergey Andreevich,
Researcher, Department for Improving the Legal Regulation of the Activities of the Criminal Executive System of the Center for the Study of Management Problems and the Organization of the Execution of Sentences in the Criminal Executive System Federal Government Research Institute of the Federal Penitentiary Service of Russia

DIGITAL TRANSFORMATION OF CRIME AND THE EVOLUTION OF RUSSIAN CRIMINOLOGICAL POLICY: VICTIMOLOGICAL AND INFORMATION-ANALYTICAL ASPECTS

Annotation. *The digitalization of social relations has transformed not only communication and economic exchange but also the mechanisms of criminal behaviour, which objectively calls for a revision of priorities within Russian criminological policy. The paper analyses key vectors of technolog-*

ical impact on crime: "hybridization" of criminal practices, the blurring of boundaries between offline and online environments, the rise of social engineering as a mass modus operandi, increasing victimological risks driven by self-disclosure in digital platforms, and the institutionalization of shadow markets in anonymous network segments. It is argued that digital traces become a universal resource for detection, proof, and prevention, yet their use is associated with risks of loss, modification, and data fragmentation, requiring standardized procedures for collection and integrity assurance. The study substantiates the перспективность of distributed ledgers for criminologically significant data accounting and of big data/AI tools for monitoring and early threat detection, provided strict legal safeguards, auditing, and accountability are ensured. Special attention is given to human resources: digital crime combines technical and socio-psychological mechanisms, necessitating interdisciplinary training and systematic prevention of digital victimization. The conclusion offers practical directions for the development of Russian criminological policy in the digital society.

Key words: *digital criminology; cybercrime; criminological policy; digital trace; social engineering; darknet; big data; artificial intelligence; cybervictimology.*

Цифровая среда стала повседневной инфраструктурой: платежи, коммуникации, получение услуг, идентификация личности и участие в публичной сфере осуществляются через платформы и сетевые сервисы. В подобных условиях криминологическая политика — как система научно обоснованных целей, принципов и мер предупреждения преступности, её причин и условий — неизбежно сталкивается с изменением криминогенных факторов и с появлением новых каналов преступного воздействия. Небольшое вступление необходимо для фиксации исходного тезиса: цифровизация не «создаёт» преступность, но трансформирует её социальные и технологические механизмы, масштабирует последствия и меняет способы выявления, доказывания и профилактики. Следовательно, требуются не частные корректировки отдельных практик, а переосмысление связки «причины и условия — профилактика — правоохранительная деятельность — общественная безопасность» с учётом цифровых реалий.

Методологически уязвимо рассматривать киберпреступность как автономный сектор. На практике цифровые каналы и цифровые следы включаются в подготовку и совершение большинства противоправных деяний: от мошенничества и вымогательства до незаконного оборота наркотических средств, экономических и коррупционных преступлений. Формируется феномен «гибридизации» — когда объект посягательства может быть традиционным (имущество, здоровье, общественная безопасность), но способы совершения, координации и сокрытия опираются на цифровые платформы, а доказательственное значение приобретают электронные данные. Такой подход согласуется с отечественными концепциями цифровой криминологии, трактующими цифровую составляющую как междисциплинарное поле, где криминологический анализ должен соединяться с пониманием социальной динамики, коммуникационных практик и технологических ограничений расследования [1; 2].

Социологическая перспектива цифрового общества позволяет уточнить причины и условия цифровой трансформации преступности. Платформенная коммуникация стимулирует публичность, непрерывное самораскрытие и накопление данных о личности: геолокации, изображений, контактов, поведенческих паттернов, покупательских привычек. Сам факт наличия цифровых сервисов усиливает зависимость человека от инфраструктуры доверия: пользователь вынужден полагаться на интерфейсы и «подсказки» системы, а не на проверяемые собственными усилиями признаки достоверности. В результате формируются новые виктимологические риски: не только прямые имущественные потери, но и репутационный ущерб, шантаж, вымогательство, давление через компрометирующие материалы. Эти механизмы соотносятся с описанием цифрового общества как единства реального и виртуального измерений, в котором цифровые практики становятся нормой социального поведения и одновременно расширяют поле уязвимостей личности [5].

Наиболее массовым механизмом современных посягательств становится социальная инженерия. Её эффективность обусловлена тем, что значительная доля преступлений строится на манипуляции доверием, авторитетом и срочностью, тогда как «техническая оболочка» (подмена номера, фишинговая форма, имитация интерфейса банка или государственного сервиса, ложные ссылки в мессенджерах) обслуживает психологический сценарий. Для криминологической политики принципиально, что социальная инженерия снижает порог входа в преступность: для результата зачастую не требуются высокие технические компетенции, зато требуется знание поведенческих закономерностей, способность управ-

лять вниманием и эмоциями потерпевшего. Следовательно, профилактика не может ограничиваться инженерно-техническими рекомендациями; она должна включать инструменты поведенческого предупреждения: обучение распознаванию манипулятивных сценариев, формирование устойчивых когнитивных «правил остановки» (отложенное решение, независимая проверка канала связи, отказ от передачи кодов/паролей), а также стандартизацию безопасного пользовательского поведения в организациях и домохозяйствах.

Актуализация кибервиктимологии особенно отчётлива на примере кибермошенничества, которое приобретает признаки социально значимого риска и затрагивает различные возрастные и социальные группы. Для разработки профилактических программ важны эмпирические виктимологические наблюдения, фиксирующие неоднородность состава потерпевших и связь виктимизации с типичными «цифровыми привычками». Показательно, что отечественные исследования дают возможность выделять устойчивые профили риска и оценивать структуру криминальной виктимности по ряду показателей, что повышает адресность профилактики и позволяет уходить от абстрактных рекомендаций [10; 11]. В практическом плане это означает необходимость перехода от универсальных информационных сообщений к сегментированной профилактике: разные группы нуждаются в разных «языках предупреждения», разной интенсивности и разном наборе защитных практик. Для молодёжи ключевой риск часто связан с коммуникационными практиками и цифровой идентичностью, для людей среднего возраста — с финансовыми сценариями и услугами, для пожилых — с доверчивостью и дефицитом навыков проверки источников.

Отдельным фактором цифровой криминализации выступают анонимизирующие технологии и формирование теневых сегментов сети, обеспечивающих устойчивое функционирование преступных рынков. Инфраструктура скрытых сервисов и криптографические механизмы создают условия для торговли персональными данными, сбыта запрещённых товаров, распространения вредоносных программ, посредничества в обналичивании и легализации доходов, предоставления «криминальных услуг». В криминологическом смысле здесь важны два обстоятельства. Во-первых, анонимность снижает риски для участников теневого рынка и повышает его устойчивость, что стимулирует специализацию и разделение ролей. Во-вторых, сетевое взаимодействие ускоряет обмен криминогенными знаниями, стандартизирует преступные «скрипты» и расширяет географию посягательств без пропорционального роста издержек. Такие процессы корреспондируют с тезисом о цифровизации и сетевизации общества постмодерна, где девиантные практики получают новые формы организации и воспроизводства [3].

При этом криминологически неверно отождествлять технологии приватности с преступностью. Анонимность может служить законным целям: защите конфиденциальности, снижению рисков преследования, обеспечению безопасности коммуникаций. Следовательно, криминологическая политика должна исходить из принципа пропорциональности вмешательства и из правовой определённости критериев, по которым государство ограничивает цифровую приватность. Иначе профилактика рискует превратиться в источник вторичных криминогенных эффектов: недоверия к институтам, ухода коммуникаций в более закрытые каналы, расширения теневых практик. Таким образом, при разработке мер противодействия преступности в анонимных сегментах сети требуется баланс: эффективное выявление и пресечение преступлений должно сочетаться с процедурами судебного контроля, ответственностью за незаконное вмешательство в приватность и прозрачными регламентами доступа к данным.

Универсальным элементом современной преступности становится цифровой след. Геолокация, сведения операторов связи, записи видеонаблюдения, данные платёжных систем, метаданные сообщений и системные журналы сервисов приобретают значение не только для раскрытия «сетевых» преступлений, но и для расследования традиционных деяний. Практика подтверждает, что для следователя критически важны навыки работы с цифровыми уликами: они позволяют устанавливать мотивы, подтверждать алиби, выявлять маршруты и контакты, восстанавливать хронологию событий. На уровне криминологической политики это меняет требования к организационным стандартам: необходимо сокращать временной разрыв между событием и фиксацией данных, унифицировать процедуру их изъятия, обеспечить непрерывность цепочки хранения и минимизировать риски модификации. Российские исследования, посвящённые расследованию интернет-преступлений и особенностям получения доказательственной информации, подчёркивают зависимость результативности от своевременности и процессуальной корректности работы с цифровыми источниками [7], а также демонстрируют, что даже в специфических сегментах (например, интернет-наркосбыт) криминалистические признаки и информационные следы позволяют выстраивать доказательственные модели при наличии надлежащих процедур [6].

Одновременно расширение цифрового доказательственного поля порождает риски: неоднородность форматов, фрагментация данных, их зависимость от коммерческих платформ и облачных сервисов, высокая скорость утраты и возможность подделки цифровых файлов. Следовательно, криминологическая политика должна включать не только технологические инициативы, но и нормативно-организационные стандарты: минимальные требования к фиксации, классификацию источников данных, регламенты взаимодействия с операторами и платформами, требования к логированию операций доступа, а также профессиональную подготовку кадров, способных оценивать достоверность и релевантность цифровых следов. Важен и виктимологический компонент: некорректное обращение с данными потерпевшего (утечка, разглашение) способно вызвать вторичную виктимизацию, снизить готовность граждан к сотрудничеству и увеличить латентность преступности.

Одним из перспективных решений проблемы целостности и неизменности данных в криминологически значимых информационных системах рассматривается использование распределённых реестров. Идея заключается не в «переносе всего» на блокчейн, а в применении его свойств (неизменяемость записей, распределённая верификация, аудит операций) для учёта и контроля жизненного цикла данных. В отечественной научной дискуссии блокчейн связывается с повышением достоверности криминологической информации и снижением рисков подделки или утраты [9]. Практически это может означать: регистрацию факта поступления цифрового носителя, фиксацию хэшей файлов, протоколирование доступа к данным, создание проверяемой истории операций. Вместе с тем криминологическая политика должна учитывать ограничения: технологические решения не заменяют процессуальных гарантий, а применение распределённых реестров требует определённости в вопросах доступа, разграничения полномочий и ответственности за внесение данных.

Важнейшее направление цифровой модернизации криминологической политики связано с большими данными и искусственным интеллектом. Мониторинг публичных информационных потоков, выявление аномалий в транзакциях и сетевой активности, автоматизированный анализ связей между событиями и субъектами способны повысить скорость обнаружения угроз и обоснованность профилактических решений [1; 2]. Однако применение алгоритмов в сфере предупреждения преступности неизбежно порождает правовые и этические риски: ложноположительные срабатывания, дискриминационные эффекты на уровне данных и моделей, непрозрачность критериев классификации, «самоисполняющиеся» прогнозы при неосторожном использовании профилирования. Поэтому криминологическая политика должна формулировать рамки допустимости алгоритмизации: обязательный аудит моделей, проверяемость данных, документирование решений, возможность оспаривания, человеческое принятие финального решения, а также ограничение использования высокорисковых систем без специального регулирования. Значимость правовых рамок цифровой безопасности подчёркивается и в отечественных работах, рассматривающих цифровую безопасность как ресурс уголовно-правового и криминологического воздействия [4].

Межведомственная интеграция выступает организационным условием эффективности. Противодействие цифровым угрозам требует согласованного обмена данными между правоохранительными органами, финансовым сектором, операторами связи и цифровыми платформами при соблюдении законодательства о персональных данных и режимов тайны. Важна не идея «неограниченного доступа», а построение стандартных протоколов реагирования: минимально необходимых наборов сведений, сроков предоставления, способов верификации, ответственных лиц и процедур контроля. Для криминологической политики это означает переход от фрагментарных ведомственных практик к согласованной архитектуре профилактики и расследования, где единые стандарты данных и единая терминология снижают транзакционные издержки и ускоряют предупреждение ущерба.

Кадровое обеспечение является ключевым фактором устойчивости политики в цифровую эпоху. Цифровая преступность сочетает технические и социально-психологические механизмы, поэтому «узкая» подготовка специалиста — только юридическая или только инженерная — оказывается недостаточной. Необходим междисциплинарный профиль: правовое регулирование цифровых прав и обращения данных, основы цифровой криминалистики и сетевой аналитики, психология принятия решений и манипулятивных технологий, базовая криптография, понимание финансовых технологий и типовых схем кибермошенничества. Подобное понимание соответствует отечественным подходам к цифровой криминологии как междисциплинарной области, в которой результативность зависит от скорости и качества обмена знаниями между юристами, специалистами по информационным технологиям и психологами [1; 3].

Наряду с профессиональной подготовкой значима массовая профилактика, ориентирован-

ная на повышение цифровой грамотности. В отличие от ряда «классических» криминогенных факторов, цифровые риски во многом модифицируемы через обучение и стандартизацию безопасных действий. Криминологическая политика в этой части должна уходить от эпизодических кампаний к устойчивым программам, встроенным в систему образования, корпоративные стандарты и пользовательские интерфейсы сервисов. Эффективны меры, меняющие «архитектуру выбора»: двухфакторная аутентификация по умолчанию, понятные предупреждения о рисках, ограничение опасных операций без дополнительной проверки, простые каналы связи для подтверждения подозрительных действий. В виктимологическом плане такие меры сокращают вероятность успеха социальной инженерии и снижают латентность, поскольку потерпевший получает понятный алгоритм действий и не опасается стигматизации.

Заключительные положения позволяют зафиксировать, что цифровая трансформация не отменяет классических закономерностей преступного поведения, но расширяет его инструментарий, усложняет организацию преступных практик и масштабирует последствия для личности и общества. Для российской криминологической политики это означает необходимость перехода к модели, в которой цифровые параметры включаются в диагностику причин и условий преступности, в виктимологическую профилактику и в технологические стандарты работы с доказательствами. Ключевые выводы сводятся к следующему: цифровизация ведёт к «гибридизации» преступности и размыванию границ между сетевыми и несетевыми формами, что требует отказа от узкого понимания киберпреступности как изолированного сегмента и внедрения сквозного учёта цифровых факторов в профилактике; социальная инженерия становится ведущим механизмом массовой виктимизации, поэтому приоритетом выступают адресные программы цифровой грамотности и поведенческой профилактики; анонимные сегменты сети формируют устойчивые теневые рынки и преступные сообщества, что актуализирует развитие криптографических компетенций и межгосударственного взаимодействия при соблюдении принципа пропорциональности вмешательства; цифровой след превращается в ключевой ресурс раскрытия и предупреждения, что требует стандартизации процедур фиксации и хранения данных и внедрения решений контроля целостности; применение больших данных и искусственного интеллекта перспективно для мониторинга и раннего выявления угроз, но должно сопровождаться правовыми гарантиями, аудитом и ответственностью за решения; кадровое обеспечение и устойчивость криминологической политики в цифровую эпоху зависят от междисциплинарной подготовки специалистов и институционализированного научно-практического взаимодействия. Реализация обозначенных направлений позволит укрепить научную обоснованность и результативность российской криминологической политики в условиях цифрового общества.

Список литературы:

[1] Ищук Я. Г., Пинкевич Т. В., Смольянинов Е. С. Цифровая криминология: учебное пособие. Москва: Академия управления МВД России, 2021. 244 с.

[2] Овчинский В. С. Криминология цифрового мира: учебник для магистратуры. Москва: Норма: ИНФРА-М, 2018. 352 с.

[3] Комлев Ю. Ю. Цифровизация, сетевизация общества постмодерна и развитие цифровой криминологии и девиантологии // Вестник Казанского юридического института МВД России. 2020. Т. 11. № 1(39). С. 31–40.

[4] Лебедев С. Я. Цифровой безопасности — цифровой уголовно-правовой ресурс // Криминология: вчера, сегодня, завтра. 2019. № 4. С. 17–25.

[5] Добринская Д. Е. Цифровое общество в социологической перспективе // Вестник Московского университета. Серия 18. Социология и политология. 2019. Т. 25. № 4. С. 175–192.

[6] Моисеев А. М., Кондратюк С. В. Криминалистические признаки наркосбыта посредством сети Интернет // Балканское научное обозрение. 2017. № 1. С. 43–46.

[7] Моисеев А. М., Кондратюк С. В. Возможности получения доказательственной информации при расследовании интернет-преступлений // Хуманитарни Балкански изследвания. 2017. № 1. С. 41–43.

[8] Кондратюк С. В. Виктимологические данные в структуре криминалистической характеристики // Вектор науки Тольяттинского государственного университета. Серия «Юридические науки». 2019. № 3(38). С. 17–22.

[9] Аносов А. В. Использование технологии блокчейн в процессе формирования и учета криминологической информации // Вестник Казанского юридического института МВД России. 2018. № 2. С. 211–216. DOI: 10.24420/KUI.2018.32.13968.

[10] Кабанов П. А. Жертвы кибермошенничества как один из объектов современной кибервиктимологии: краткий статистический анализ показателей криминальной виктимности 2021–2022 гг. // Виктимология. 2023. Т. 10. № 1. С. 17–28. DOI: 10.47475/2411-0590-2023-10102.

[11] Антонян Е. А., Клещина Е. Н. Кибервиктимность // Вестник Пермского института ФСИН России. 2019. № 3. С. 5–10.

References:

[1] Ishchuk Y. G., Pinkevich T. V., Smolyaninov E. S. Digital criminology: a textbook. Moscow: Academy of Management of the Ministry of Internal Affairs of Russia, 2021. 244 pp.

[2] Ovchinsky V. S. Criminology of the digital world: a textbook for a master's degree. Moscow: Norm: INFRA-M, 2018. 352 pp.

[3] Komlev Yu. Yu. Digitalization, networking of postmodern society and the development of digital criminology and deviantology//Bulletin of the Kazan Law Institute of the Ministry of Internal Affairs of Russia. 2020. T. 11. № 1(39). S. 31-40.

[4] Lebedev S. Ya. Digital security - digital criminal law resource//Criminology: yesterday, today, tomorrow. 2019. № 4. S. 17-25.

[5] Dobrinskaya D.E. Digital Society in a Sociological Perspective//Bulletin of Moscow University. Series 18. Sociology and political science. 2019. VOL. 25. № 4. S. 175-192.

[6] Moiseev A.M., Kondratyuk S.V. Forensic signs of drug trafficking via the Internet//Balkan Scientific Review. 2017. № 1. S. 43-46.

[7] Moiseev A.M., Kondratyuk S.V. Possibilities of obtaining evidentiary information in the investigation of Internet crimes//Humanitarni Balkan research. 2017. № 1. S. 41-43.

[8] Kondratyuk S.V. Victimological data in the structure of forensic characteristics//Vector of Science of Togliatti State University. "Legal Sciences" series. 2019. № 3(38). S. 17-22.

[9] A. V. Anosov. Use of blockchain technology in the process of formation and accounting of criminological information//Bulletin of the Kazan Law Institute of the Ministry of Internal Affairs of Russia. 2018. № 2. S. 211-216. DOI: 10.24420/KUI.2018.32.13968.

[10] Kabanov P. A. Victims of cyber fraud as one of the objects of modern cybervictimology: a brief statistical analysis of criminal victimization indicators 2021-2022//Victimology. 2023. T. 10. № 1. S. 17-28. DOI: 10.47475/2411-0590-2023-10102.

[11] Antonyan E.A., Kleshchina E.N. Cybervictimity//Bulletin of the Perm Institute of the Federal Penitentiary Service of Russia. 2019. № 3. S. 5-10.