Научная статья
https://doi.org/10.34853/NZ.2026.42.82.002

УДК 343

Безсонова Алевтина Олеговна
студент ФГБОУ ВО «Кубанский государственный аграрный университет им. И.Т. Трубилина».
E-mail: alevtinabezsonova@gmail.com
Alevtina O. Bezsonova
student of the Kuban State Agrarian University" them. I.T. Trubilina
Email: alevtinabezsonova@gmail.com

ВЛИЯНИЕ ЦИФРОВИЗАЦИИ НА УГОЛОВНОЕ ПРАВО И УГОЛОВНЫЙ ПРОЦЕСС

THE IMPACT OF DIGITALIZATION ON CRIMINAL LAW AND CRIMINAL PROCEDURE

Аннотация: *В настоящей статье анализируется влияние цифровизации на уголовное право и процесс. Рассматривается несовершенство процессуального режима цифровых доказательств, их статус в Уголовно-процессуальном Кодексе Российской Федерации и риски нарушения принципа допустимости. Исследуется появление новых форм киберпреступности, таких как криптопреступность и использование «дипфейков». Делается вывод о необходимости создания специального правового режима для цифровых доказательств и модернизации уголовного и уголовно-процессуального законодательства.*

Ключевые слова: *цифровизация, уголовный процесс, цифровые доказательства, киберпреступность, допустимость, уголовно-процессуальное право, уголовный закон, криминализация.*

Abstract: *This article analyzes the impact of digitalization on criminal law and procedure. It examines the imperfections of the procedural regime for digital evidence, its status in the Criminal Procedure Code of the Russian Federation, and the risks of violating the admissibility principle. The emergence of new forms of cybercrime, such as cryptocrime and the use of deepfakes, is examined. A conclusion is reached regarding the need to create a special legal regime for digital evidence and modernize criminal and criminal procedure legislation.*

Keywords: *digitalization, criminal procedure, digital evidence, cybercrime, admissibility, criminal procedure law, criminal law, criminalization.*

Цифровые технологии проникли уже практически во все сферы жизни человека, их влияние мы также можем наблюдать и в системах права, в том числе уголовного и уголовно-процессуального. Нельзя однозначно ответить, носит данный процесс положительный или отрицательный характер, он довольно противоречив, так как, с одной стороны, цифровые технологии являются действенным инструментом в руках правоприменителя, с другой - порождают принципиально новые формы противоправного поведения и создают серьезные процессуальные барьеры.

Настоящая статья сосредоточена на двух ключевых аспектах этой проблематики: эволюции цифровых доказательств в уголовном судопроизводстве и криминализации новых форм киберпреступности. Анализ проводится с опорой на действующий Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации с учетом тенденций в зарубежном законодательстве и доктрине.

Интересен процессуальный статус цифровых доказательств и проблема их допустимости.

Понятие «доказательства» в уголовном процессе закрепляется в ст. 74 УПК РФ, также там перечислен перечень того, что может использоваться в качестве доказательств, в основном это материальные носители информации, помимо различных показаний, заключений эксперта. Цифровая эра поставила под сомнение эту концепцию. Цифровая информация (электронные письма, данные с метатегами, логи серверов, сообщения из мессенджеров, файлы из облачных хранилищ) не является вещью в классическом понимании. Она копируема, мультиплицируема, подвержена изменению без видимых следов и неотделима от устройства и программного обеспечения, с помощью которых и воспроизводится.

Несмотря на это, законодатель, по сути, подвел цифровые данные под существующие классификации. Чаще всего они признаются иными документами (ст. 84 УПК РФ) или вещественными доказательствами, если на носитель информации было оказано преступное воздействие или он сохранил следы преступления[1]. Однако такая подмена понятий создает практические сложности. Требования к протоколу осмотра вещественного доказательства (ст. 180 УПК РФ) плохо применимы к осмотру информации на жестком диске, который требует специальных познаний и использования сложного программного обеспечения. Процесс изъятия цифрового носителя, его исследования и приобщения к делу должен обеспечивать главное – сохранение целостности данных и возможность проверки их подлинности.

Ключевой проблемой становится допустимость цифровых доказательств. Гарантией допустимости выступает соблюдение процедуры, которая подтверждает, что представленные данные являются теми же самыми, что и были получены с исходного носителя, и не были сфальсифицированы. Для этого требуется выстраивание четкой «цепочки доказательств», документально фиксирующей каждое лицо, имевшее доступ к носителю или

данным, время и цели такого доступа. В российском процессе этот подход формально не закреплен, что создает риски для сторон обвинения и защиты. Защита, в свою очередь, сталкивается с трудностями в проведении самостоятельной экспертизы, если исходный носитель изъят и хранится у следствия, а копия, предоставленная защите, не была надлежащим образом заверена.

Отдельный вызов – доказательства из облачных сред и зарубежных сервисов. Юрисдикция над данными, физически расположенными на серверах в другой стране, порождает коллизии международного права. Получение таких доказательств через процедуру правовой помощи часто является длительным и неэффективным, что провоцирует правоохранительные органы на использование негласных методов сбора информации, допустимость которой в суде может быть оспорена.

Рассмотрим также проблемы и коллизии, возникшие в уголовном законодательстве с развитием цифровых технологий и появлением киберпреступности.

В цифровой среде совершается множество преступлений, они продолжают модернизироваться и преображаться ежедневно, поэтому, конечно действующий Уголовный Кодекс Российской Федерации, несмотря на то, что содержит отдельную главу, посвященную преступлениям в сфере компьютерной информации, не охватывает все виды общественно-опасных деяний в данной области[2].

Во-первых, наблюдается тенденция «гибридизации» преступлений. Традиционные составы, такие как мошенничество (ст. 159 УК РФ), вымогательство (ст. 163 УК РФ), клевета (ст. 128.1 УК РФ), все чаще совершаются с исключительным использованием цифровых средств[3]. Квалификация по правилам совокупности преступлений не всегда отражает повышенную общественную опасность и специфику такого деяния. Массовость и анонимность, предоставляемые интернетом, трансформируют сам способ исполнения преступления, делая его более опасным.

Во-вторых, возникают качественно новые деяния, не укладывающиеся в существующие составы. К ним можно отнести:

- криптопреступность: незаконные действия, связанные с использованием криптовалют и технологий блокчейна для мошенничества, хищения средств, отмывания денег, финансирования терроризма или продажи запрещенных товаров и услуг;

- преступления против личности в цифровой среде: кибersталкинг, доксинг (публикация персональных данных с целью травли), дипфейки (незаконное использование чужого лица или голоса без согласия для дальнейшего распространения), используемые для шантажа, компрометации или подрыва доверия[4]. Существующие составы об угрозах или нарушении неприкосновенности частной жизни часто не покрывают весь спектр вреда, причиняемого такими действиями.

- преступное использование данных и алгоритмов: дискриминация или манипулирование поведением людей на основе алгоритмического анализа данных, совершенные не государством, а коммерческой организацией.

В-третьих, остро стоит проблема экстерриториальности. Установление субъекта преступления, действующего под псевдонимом через анонимные сети, и привлечение его к ответственности требует беспрецедентного уровня международного сотрудничества, который на данный момент недостаточно развит.

Цифровизация не является временным трендом, это новая реальность, требующая системного переосмысления уголовно-правовых и процессуальных институтов. На основании проведенного анализа можно сформулировать следующие выводы и предложения:

1. В уголовно-процессуальном праве необходима легализация специального правового режима для цифровых доказательств. Целесообразно ввести в УПК РФ отдельную статью, определяющую понятие «цифровое доказательство», и детально регламентировать процедуры его изъятия, копирования, исследования, хранения и представления в суд. Ключевым элементом должно стать законодательное закрепление требований к обеспечению «цепочки доказательств» и использованию криптографических методов проверки целостности.

2. В уголовном праве требуется развитие и дифференциация ответственности за киберпреступления[5].

Введение квалифицирующих признаков для традиционных составов преступлений, указывающих на совершение их с использованием информационно-телекоммуникационных сетей, включая интернет, в крупном или особо крупном размере, либо в отношении широкого круга лиц.

Криминализация новых общественно опасных форм поведения: создание и распространение дипфейков с преступными целями; доксинг, повлекший тяжкие последствия; вмешательство в работу алгоритмов искусственного интеллекта, управляющих критической инфраструктурой.

Уточнение и расширение формулировок в главе 28 УК РФ с учетом современных технологий (например, четкое определение понятия «криптографические средства»).

3. На международном и межведомственном уровне необходимо ускорение процессов совершенствования законодательства в сфере киберпреступности и выработки упрощенных, но легитимных механизмов получения цифровых доказательств за рубежом. Важным шагом является развитие собственных цифровых компетенций у следователей, прокуроров и судей, включая понимание базовых принципов работы сетей, шифрования и блокчейна.

Цифровизация ставит перед уголовным правом и процессом фундаментальный вопрос о балансе между эффективностью борьбы с преступностью и защитой прав личности (включая право на неприкосновенность част-

ной жизни и защиту данных). Разрешение этого вопроса возможно только через четкое, технологически грамотное и соразмерное законодательное регулирование, которое будет не догонять, а опережать вызовы цифровой эпохи.

Источники:

1. Уголовно-процессуальный кодекс Российской Федерации : федер. закон от 18.12.2001 №174-ФЗ : в ред. от 15.12.2025 // СЗ РФ. – 2001. – № 52(ч.1). – Ст. 4921. / http://pravo.gov.ru - 15.12.2025.

2. Матвеев И.В. Взаимовлияние цифровых технологий и уголовного права // Закон и право. – 2024. – № 7. – С. 179-182.

3. Уголовный кодекс Российской Федерации : федер. закон. от 13.06.1996 № 63-ФЗ : в ред. от 17.11.2025 // СЗ РФ. – 1996. – № 25. – Ст. 2954. / http://pravo.gov.ru - 17.11.2025.

4. Воронин И.А., Гавра Д.П. Дипфейки, современное понимание, подходы к определению, характеристики, проблемы и перспективы // Российская школа связей с общественностью. – 2024. – № 33. – С. 28-47.

5. Вилисова И.Б. Предотвращение киберпреступлений согласно УК РФ // Восточно-европейский научный журнал. – 2022. – № 9. – С. 35-38.

1. Criminal Procedure Code of the Russian Federation: federal law of 18.12.2001 No. 174-FZ: as amended on 15.12.2025 // Collected Legislation of the Russian Federation. – 2001. – No. 52 (Part 1). – Art. 4921. / http://pravo.gov.ru - 15.12.2025.

2. Matveyev I.V. Interaction of Digital Technologies and Criminal Law // Law and Right. – 2024. – No. 7. – P. 179-182.

3. Criminal Code of the Russian Federation: federal law of 13.06.1996 No. 63-FZ: as amended on 17.11.2025 // Collected Legislation of the Russian Federation. – 1996. – No. 25. – Art. 2954. / http://pravo.gov.ru - 17.11.2025.

4. Voronin I.A., Gavra D.P. Deepfakes: modern understanding, approaches to definition, characteristics, problems and prospects // Russian School of Public Relations. – 2024. – No. 33. – P. 28-47.

5. Vilisova I.B. Prevention of cybercrimes according to the Criminal Code of the Russian Federation // East European Scientific Journal. - 2022. - No. 9. - P. 35-38.

Sources:

1. The Criminal Procedure Code of the Russian Federation : Federal Law. The law of December 18, 2001 No. 174-FZ : as amended. dated 12/15/2025 // Federal Law of the Russian Federation. – 2001. – No. 52 (part 1). – Article 4921. / http://pravo.gov.ru - 12/15/2025.

2. Matveev I.V. The mutual influence of digital technologies and criminal law // Law and Law. – 2024. – No. 7. – pp. 179-182.

3. The Criminal Code of the Russian Federation: feder. law. dated 13.06.1996 No. 63-FZ : as amended . dated 11/17/2025 // Federal Law of the Russian Federation. – 1996. – No. 25. – V. 2954. / http://pravo.gov.ru - 11/17/2025.

4. Voronin I.A., Gavra D.P. Deepfakes, modern understanding, approaches to definition, characteristics, problems and prospects // Russian School of Public Relations. – 2024. – No. 33. – pp. 28-47.

5. Vilisova I.B. Prevention of cybercrimes according to the Criminal Code of the Russian Federation // Eastern European Scientific Journal. – 2022. – No. 9. – pp. 35-38.

1. The Criminal Procedure Code of the Russian Federation: Federal Law No. 174-FZ dated December 18, 2001: as amended on December 15, 2025 // Collection of Legislation of the Russian Federation. – 2001. – No. 52 (part 1). – Article 4921. / http://pravo.gov.ru - 12/15/2025.

2. Matveev I.V. Interaction of digital technologies and criminal law // Law and Law. – 2024. – No. 7. – pp. 179-182.

3. Criminal Code of the Russian Federation: Federal Law of 13.06.1996 No. 63-FZ: as amended on 17.11.2025 // Collection of legislation of the Russian Federation. – 1996. – No. 25. – Article 2954. / http://pravo.gov.ru - 11/17/2025.

4. Voronin I.A., Gavra D.P. Fakes: modern understanding, approaches to definition, characteristics, problems and prospects // Russian School of Public Relations. - 2024. – No. 33. – pp. 28-47.

5. Vilisova I.B. Prevention of cybercrimes in accordance with the Criminal Code of the Russian Federation // East European Scientific Journal. - 2022. - No. 9. - pp. 35-38.