УДК 34 **DOI: 10.34670/AR.2025.59.77.024**

Противодействие преступности в цифровом пространстве: анализ современного состояния

Новиков Алексей Валерьевич

Доктор педагогических наук, кандидат юридических наук, профессор;
Член Союза журналистов России (Московское региональное отделение);
главный научный сотрудник,
Научно-исследовательский институт Федеральной службы исполнения наказаний России,
125130, Российская Федерация, Москва, ул. Нарвская, 15-а;
профессор кафедры уголовного права и правоохранительной деятельности,
Астраханский государственный университет,
414056, Российская Федерация, Астрахань, ул. Татищева, 20-а;
e-mail: novikov.pravo@mail.ru

Дакашев Иса Хамзатович

Преподаватель кафедры уголовно-правовых дисциплин,
Самарский юридический институт Федеральной службы исполнения наказаний России,
443022, Российская Федерация, Самара, ул. Рыльская, 24-в;
e-mail: alikov1964@mail.ru

Слабкая Диана Николаевна

Старший научный сотрудник,
Научно-исследовательский институт Федеральной службы исполнения наказаний России,
125130, Российская Федерация, Москва, ул. Нарвская, 15-а;
e-mail: sdn10.70@mail.ru

Аннотация

В статье рассматривается проблема преступности в цифровом пространстве, внимание уделяется ее специфике и влиянию на деятельность уголовно-исполнительной системы России. Проводится анализ современного состояния киберпреступности, включая наиболее распространенные виды преступлений и методы их совершения. Исследуются факторы, способствующие распространению преступности в цифровой среде, в частности, анонимность, глобальность и доступность информационных технологий. Рассматриваются правовые основы противодействия киберпреступности в России, в том числе соответствующие статьи Уголовного кодекса РФ и Уголовно-исполнительного кодекса РФ. Анализируются существующие механизмы и методы противодействия киберпреступности в России, выявляются их сильные и слабые стороны. Предлагаются конкретные рекомендации по совершенствованию системы противодействия преступности в цифровом пространстве, направленные на повышение эффективности профилактики, выявления, раскрытия и расследования киберпреступлений, а также на обеспечение информационной безопасности учреждений УИС.

Для цитирования в научных исследованиях

Новиков А.В., Дакашев И.Х., Слабкая Д.Н. Противодействие преступности в цифровом пространстве: анализ современного состояния // Вопросы российского и международного права. 2025. Том 15. № 11А. С. 208-216. DOI: 10.34670/AR.2025.59.77.024

Ключевые слова

Киберпреступность, цифровое пространство, уголовно-исполнительная система, информационная безопасность, противодействие преступности, Уголовно-исполнительный кодекс, профилактика киберпреступлений, информационные технологии, осужденные, интернет.

Введение

Цифровое пространство, став неотъемлемой частью современной жизни, предоставляет колоссальные возможности для коммуникации, бизнеса и доступа к информации. Однако, вместе с тем, оно порождает и новые формы преступности, требующие комплексного и эффективного противодействия. Преступления в цифровой сфере наносят значительный ущерб гражданам, бизнесу и государству, подрывая доверие к технологиям и замедляя развитие цифровой экономики. Определенную актуальность данная проблема приобретает в контексте уголовно-исполнительной системы (далее – УИС) России, где процессы цифровизации идут полным ходом, затрагивая как управление учреждениями, так и реабилитацию осужденных [Ананьева, 2025]. Внедрение информационных технологий в пенитенциарную сферу предоставляет новые возможности для оптимизации административных процедур, повышения эффективности надзора и контроля, а также для предоставления осужденным доступа к образовательным и реабилитационным программам, основанным на современных цифровых решениях.

Однако, вместе с очевидными преимуществами, цифровизация УИС порождает и ряд серьезных рисков, связанных с информационной безопасностью и защитой персональных данных [Силантьева, 2025]. Данное может касаться в том числе и информации об осужденных, которая, в силу своей специфики, является крайне чувствительной и подвержена риску несанкционированного доступа, модификации или раскрытия. Утечка такой информации может иметь катастрофические последствия для самих осужденных, так и для их семей.

Кроме того, цифровизация предполагает широкое использование компьютерных сетей, баз данных и облачных технологий, которые, в свою очередь, подвержены кибератакам со стороны злоумышленников. Успешные кибератаки на информационные системы УИС могут привести к нарушению работы учреждений, компрометации данных, а также к созданию угрозы для жизни и здоровья осужденных и сотрудников.

В связи с этим, обеспечение информационной безопасности и защиты персональных данных в УИС становится одной из приоритетных задач, требующих комплексного и системного подхода [Овчинников, 2025]. В этой связи востребовано перманентно дорабатывать и внедрять эффективные меры по предотвращению несанкционированного доступа к информации, защите от киберугроз, а также по обеспечению конфиденциальности и целостности данных, что предполагает, в частности, повышение квалификации сотрудников УИС в области

информационной безопасности, внедрение современных технологий защиты информации, а также доработку и реализацию строгих процедур доступа и контроля за использованием информационных систем.

Основное содержание

Цифровизация общества, несомненно положительно влияет на жизнедеятельность человека, повышает качество его жизни путем доступа к самому разнообразному спектру информационных ресурсов. Однако, внедрение информационно-коммуникационных технологий в различные сферы общественных отношений используется преступниками для совершения противоправных деяний.

Анализ характера и особенностей криминальной активности в цифровом пространстве, позволяет констатировать, что субъектами такой активности могут выступать как лица, не обладающие определенными информационно-технологическими умениями и навыками, так и лица, относящиеся к категории профессиональных IT-преступников. Изучение факторов, способствующих совершению преступлений в цифровом пространстве позволяет сформулировать меры, направленные на нейтрализацию рассматриваемого противоправного явления.

Преступность в цифровом пространстве – это собирательное понятие, включающее широкий спектр противоправных деяний, совершаемых с использованием информационных технологий. Эти преступления характеризуются трансграничностью, высокой латентностью и сложностью расследования. Среди наиболее распространенных видов в целом можно выделить:

– хищения денежных средств, в том числе с использованием вредоносного программного обеспечения для получения доступа к банковским счетам и картам;
– мошенничество и обманные схемы в интернете, связанные с торговлей, инвестициями, благотворительностью и другими сферами;
– распространение экстремистских и террористических материалов, вербовка новых членов, финансирование террористической деятельности;
– использование сети Интернет для организации сбыта и распространения запрещенных веществ и предметов;
– незаконное копирование, распространение и использование объектов интеллектуальной собственности.

Эти преступления не только наносят прямой финансовый или моральный ущерб жертвам, но и подрывают доверие к цифровым технологиям, создают атмосферу неопределенности и неуверенности.

В современном мире цифровые технологии прочно вошли во все сферы жизни общества, включая деятельность государственных органов и учреждений, в том числе уголовно-исполнительной системы России. Вместе с расширением возможностей, предоставляемых цифровыми технологиями, возрастает и риск совершения преступлений в цифровом пространстве. Как уже отмечалось, киберпреступность представляет собой серьезную угрозу для информационной безопасности, финансовой устойчивости и общественной стабильности. В контексте УИС России, преступления в цифровой среде создают дополнительные риски, связанные с возможностью совершения противоправных действий осужденными, обеспечением безопасности учреждений и поддержанием правопорядка.

Преступность в цифровом пространстве представляет собой новое и динамично развивающееся негативное явление, связанное с использованием информационно-коммуникационных технологий (далее – ИКТ) для совершения незаконных деяний. Сущность такого негативного явления обусловлена возможностями компьютера и компьютерных сетей, которые создают принципиально новую среду для криминальной активности – цифровая среда [Козаев, 2024].

Гаджиев Х.А. рассматривает цифровую среду как виртуальное пространство, включающее всю совокупность коммуникаций, интеракций и информационных потоков, формируемых цифровыми технологиями (компьютерными и мобильными устройствами, а также иными средствами конструирования виртуальной и дополненной реальности) [Гаджиев, 2022].

Цифровая преступность за последние годы стала серьезной проблемой мирового уровня, наносящей ущерб общественным отношениям практически во всех сферах общества и государства. Так, в соответствии со статистическими данными МВД РФ, в 2024 г. на территории России было совершено 765 тыс. преступлений цифрового характера, что на 13,1% больше, чем за аналогичный период 2023 г. Их удельный вес в общем числе преступлений за последние пять лет вырос с 25 % (2020 г) до 40% (2024 г.) [www].

Результаты исследования характера и особенностей совершения преступлений в цифровом пространстве позволяет классифицировать субъектов данных противоправных деяний на две группы:

1) преступления, совершаемые в цифровой среде лицами, не обладающими определенными информационно-технологическими умениями и навыками. К этой группе можно отнести преступления общего характера (незаконный оборот наркотиков, кражи, мошенничества и т.д.);

2) цифровые преступления, которые может совершить только лицо, обладающее определенными информационно-технологическими умениями и навыками. Сюда можно отнести: неправомерный доступ к компьютерной информации; создание, использование и распространение вредоносных компьютерных программ и т. д.

По мнению Бессонова А.А., в последние годы преступники начали активно использовать виртуальное пространство для совершения самого широкого спектра криминальных деяний: корыстной направленности, терроризма и экстремизма, преступлений против жизни и здоровья, свободы, чести и достоинства личности, половой неприкосновенности и половой свободы, незаконного оборота наркотиков и оружия и т.д [Бессовнов, 2020].

Анализ криминальной активности в киберпространстве позволяет выделить две основные закономерности:

– первое: сложность и масштабность преступлений, совершаемых «IT-преступниками» в цифровой среде, заставляет их объединяться в преступные группировки, что способствует развитию организованной преступности в киберпространстве;
– второе: происходит передел киберпространсва среди криминальных группировок, которые рассматривают такую среду как возможность организации конспиративной противоправной деятельности и незаконного обогащения финансовыми средствами за короткий отрезок время [Осипенко, 2017].

В связи с этим, перед наукой и правоприменительной практикой стоит задача объяснить особенности современной киберпреступности, спрогнозировать ее уровни с целью создания эффективной инструментарий поиска и обработки различных информационных данных, в том числе и о личности киберпреступника [Smith, 2017].

Основными факторами, способствующими совершению преступлений в цифровом пространстве выступают:

– использования цифровой среды в целях конспирации;
– использование ресурсов киберпространства для криминальной пропаганды (распространение криминальной субкультуры, вовлечение молодежи в преступную среду и т.д);
– возможность использования киберпространства для дискредитации субъектов гражданско-правовых отношений, через дезинформацию и опубликования несоответствующей информации;
– использование криптовалют для «отмывания» незаконно полученных доходов;
– использование киберпространства для «криминальной разведки»;
– организация противодействия правоохранительным органам;
– высокая скорость передачи данных и мобильность цифровой среды обеспечивает оперативну. координацию противоправной деятельности киберпреступников не зависимо от места нахождения [Кобец, 2017].

С одной стороны, как уже было сказано выше, современные преступники, осознавая высокую доходность и законспиративность преступной деятельности с использованием IT-технологий, в последние годы переводят свою криминальную активность в киберсреду. При этом, такая активность включает себя: дистанционный характер совершаемых преступлений; сложный интеллектуальный характер реализуемых противоправных действий; использование высокотехнологичного оборудования и современного программного обеспечения; применение особых способов сокрытия следов преступления; отсутствие явных признаков преступного воздействия на информационную систему [Бавсун, 2019].

С другой стороны, сложившаяся и постоянно трансформирующаяся цифровая среда содержит огромный котнент информации, что безусловно способствует криминальной активности.

Необходимость повышения эффективности и результативности противодействия цифровой преступности обуславливает переориентацию оперативных подразделений правоохранительных органов с автономных ОРМ на комплексное использование средств и сил, в том числе в сети интернет и киберпространстве [ОРД в цифровом мире]. Для более эффективной и отлаженной работы по реализации совместных профилактических мероприятий, направленных на нейтрализацию криминальной активности рассматриваемой категории лиц в цифровом пространстве предлагается усилить меры, направленные на:

1. Развитие отечественного производства технических, коммуникационных средств и организационно-методического обеспечения в сфере противодействии киберпреступности. Важную роль в этом должны сыграть специалисты и ученые научно-исследовательских институтов в разработке, например, практических рекомендаций, методических пособий и иной научной продукции для практических сотрудников правоохранительных органов.

2. Подготовку квалифицированных специалистов правоохранительных органов по противодействию киберпреступности. Этому должны способствовать ведомственные образовательные организации высшего образования (далее – ОО ВО), готовящих будущих сотрудников. Отметим, что успешно функционирует Воронежский институт ФСИН России, который обеспечивает подготовку специалистов в том числе по ОП ВО 11.05.04 «Инфокоммуникационные технологии и системы специальной связи». Тем не менее в целом по

ОО ВО целесообразно расширить образовательные программы путем введения дополнительных дисциплин или курсов по противодействию преступности в цифровом пространстве.

3. Разработку комплексных программ по внедрению искусственного интеллекта для решения оперативно значимой задачи по противодействию киберпреступности. В настоящее время данное направление эффективно применяется в банковской деятельности по внедрению искусственного интеллекта для защиты банковских счетов и другой информации своих клиентов (автоматическое распознавание владельца карты, автоматическая блокировка карты при подозрительной операции и т. д.).

В настоящее время основы противодействия киберпреступности в России определены следующими нормативными правовыми актами:

Уголовный кодекс РФ: содержит статьи, предусматривающие ответственность за совершение преступлений в сфере компьютерной информации (ст. 272-274.1 УК РФ), а также за отдельные виды киберпреступлений, такие как мошенничество (ст. 159 УК РФ), вымогательство (ст. 163 УК РФ) и другие.

Уголовно-исполнительный кодекс РФ: регулирует порядок исполнения наказаний, связанных с ограничением свободы граждан, совершивших преступления в сфере компьютерной информации. В частности, в соответствии со ст. 11 УИК РФ, осужденные обязаны соблюдать требования информационной безопасности.

Федеральный закон Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ, как следует из названия устанавливает правовые основы информационной безопасности и защиты информации.

Стратегия национальной безопасности Российской Федерации: определяет основные направления обеспечения национальной безопасности, в том числе в информационной сфере.

Заключение

Эффективная борьба с киберпреступностью требует комплексного подхода, включающего в себя технические, организационные, правовые и профилактические меры. Противодействие преступности в цифровом пространстве является одной из важнейших задач, успешное решение которой требует системного решения, включающего техническое оснащение, повышение квалификации персонала, профилактическую работу с осужденными и взаимодействие с правоохранительными органами. Реализация предложенных мер позволит повысить эффективность противодействия преступности в цифровом пространстве в УИС России, обеспечить безопасность информационных ресурсов и защитить права и законные интересы осужденных и сотрудников.

Библиография

1. Ананьева Е.О. Цифровая трансформация УИС // Аграрное и земельное право. 2025. № 3. С. 209-211. http://doi.org/10.47643/1815-1329_2025_3_209.
2. Бавсун М. В. Киберпреступность как закономерный продукт современного общества // Всероссийский криминологический журнал. 2019. № 2. С. 15–17;
3. Бессонов А.А. Цифровая криминалистическая модель преступления как основа противодействия киберпреступности // Академическая мысль. 2020. № 4 (13). С. 59;
4. Габараев, А. Ш. Информационная безопасность на современном этапе гибридных войн / А. Ш. Габараев, А. В. Новиков, Д. Н. Слабкая // Вопросы российского и международного права. – 2024. – Т. 14, № 10-1. – С. 50-58. – EDN VBSJCE.

5. Гаджиев Х.А. Цифровое пространство и политическая стабильность России // Социально-политические науки. 2022. Т. 12. № 6. С. 22–28;
6. Козаев Н.Ш. Киберпреступность в современном мире: тенденции, вызовы и стратегии противодействия // Гуманитарные, социально-экономические и общественные науки, №. 11, 2024, С. 146-153;
7. Кобец П. Н. Влияние глобализации и киберпреступности на сращивание организованной преступности с радикальными террористическими и насильственными экстремистскими группами // Матрица научного познания. 2017. № 5. С. 45–47;
8. Костарев, Д. Ф. Совершенствование деятельности исправительных учреждений уголовно-исполнительной системы по обеспечению надзора за лицами, отбывающими наказание / Д. Ф. Костарев, А. В. Новиков // Вопросы российского и международного права. – 2022. – Т. 12, № 10-1. – С. 616-624. – DOI 10.34670/AR.2022.62.17.059.
9. Овчинников С. Н. Применение цифровых технологий в сфере исполнения уголовных наказаний: направления, инновации, риски // Пенитенциарная наука.2025. Т. 19, № 3 (71). С. 261–269. doi 10.46741/2686-9764.2025.71.3.004
10. Оперативно-розыскная деятельность в цифровом мире: сборник научных трудов/ под ред. В.С. Овчинского. – Москва: ИНФРА-М,2021. – С. 346;
11. Осипенко, А. Л. Организованная преступная деятельность в киберпространстве: тенденции и противодействие / А. Л. Осипенко // Юридическая наука и практика: Вестник Нижегородской академии МВД России. – 2017. – № 4(40). – С. 181-188. – EDN ZXRFTZ.
12. Серебренникова А. В. Цифровизация исполнения наказания: состояние и перспективы / А. В. Серебренникова // Человек: преступление и наказание. – 2021. – Т. 29. – № 1. – С. 40-45.
13. Силантьева Н. А. Цифровой контроль в уголовно-исполнительной системе: перспективы и вызовы внедрения новых технологий // Вестник Прикамского социального института. 2025. № 1 (100). С. 53–62.
14. Слабкая, Д. Н. К вопросу о классификации наказаний, применяемых в уголовном законодательстве России / Д. Н. Слабкая, А. В. Новиков // Вопросы российского и международного права. – 2022. – Т. 12, № 7-1. – С. 198-203. – DOI 10.34670/AR.2022.41.36.023. – EDN TMHHTM.
15. Суходолов, А.П., Иванцов, С.В., Молчанова Т.В., 2018. Цифровая криминология: математические методы прогнозирования // Всероссийском криминологическом журнале. Т. 12. № 2. С. 230–236;
16. Состояние преступности в Российской Федерации за январь - декабрь 2024 года. Официальный сайт Министерства внутренних дел Российской Федерации: https://xn--b1aew.xn--p1ai/reports/item/60248328 (Дата обращения 12.11.2025 г.).
17. Smith, G.J.D., 2017. The challenges of doing criminology in the big data era: towards a digital and data-driven approach // British Journal of Criminology. Vol. 57, iss. 2. P. 259-274.

Countering Crime in Digital Space: Analysis of the Current State

Aleksei V. Novikov

Doctor of Pedagogy, PhD in Law, Professor;
Member of the Russian Union of Journalists (Moscow regional branch);
Chief Researcher,
Scientific-Research Institute of the Federal Penitentiary Service of the Russian Federation,
125130, 15-a, Narvskaya str., Moscow, Russian Federation;
Professor of the Department of Criminal Law and Law Enforcement, Astrakhan State University,
414056, 20-a, Tatishcheva str., Astrakhan, Russian Federation;
e-mail: novikov.pravo@mail.ru

Isa Kh. Dakashev

Lecturer, Department of Criminal Law Disciplines,
Samara Law Institute of the Federal Penitentiary Service of the Russian Federation,
443022, 24-v, Rylskaya str., Samara, Russian Federation;
e-mail: alikov1964@mail.ru

Diana N. Slabkaya

Senior Researcher,
Scientific-Research Institute of the Federal Penitentiary Service of the Russian Federation,
125130, 15-a, Narvskaya str., Moscow, Russian Federation;
e-mail: sdn10.70@mail.ru

Abstract

The article addresses the problem of crime in digital space, with attention given to its specifics and impact on the activities of the Russian penal correction system. An analysis of the current state of cybercrime is conducted, including the most common types of crimes and methods of their commission. Factors contributing to the spread of crime in the digital environment are investigated, particularly anonymity, global reach, and the accessibility of information technologies. The legal foundations for countering cybercrime in Russia are considered, including relevant articles of the Criminal Code of the Russian Federation and the Penal Correction Code of the Russian Federation. Existing mechanisms and methods for countering cybercrime in Russia are analyzed, identifying their strengths and weaknesses. Specific recommendations are proposed for improving the system of countering crime in digital space, aimed at enhancing the effectiveness of prevention, detection, investigation, and prosecution of cybercrimes, as well as ensuring information security for institutions of the penal correction system.

For citation

Novikov A.V., Dakashev I.Kh., Slabkaya D.N. (2025) Protivodeystviye prestupnosti v tsifrovom prostranstve: analiz sovremennogo sostoyaniya [Countering Crime in Digital Space: Analysis of the Current State]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Matters of Russian and International Law], 15 (11A), pp. 208-216. DOI: 10.34670/AR.2025.59.77.024

Keywords

Cybercrime, digital space, penal correction system, information security, countering crime, Penal Correction Code, cybercrime prevention, information technologies, convicts, internet.

References

1. Anan'eva, E.O. (2025) Tsifrovaia transformatsiia UIS [Digital transformation of the penal system]. *Agrarnoe i zemel'noe pravo* [Agrarian and Land Law], (3), 209–211. http://doi.org/10.47643/1815-1329_2025_3_209
2. Bavsun, M.V. (2019). Kiberprestupnost' kak zakonomernyi produkt sovremennogo obshchestva [Cybercrime as a natural product of modern society]. *Vserossiiskii kriminologicheskii zhurnal* [All-Russian Criminology Journal], (2), 15–17.
3. Bessonov, A.A. (2020). Tsifrovaia kriminalisticheskaia model' prestupleniia kak osnova protivodeistviia kiberprestupnosti [Digital forensic model of crime as a basis for countering cybercrime]. *Akademicheskaia mysl'* [Academic Thought], 4(13), 59–63.
4. Gabaraev, A.Sh., Novikov, A.V., & Slabkaia, D.N. (2024). Informatsionnaia bezopasnost' na sovremennom etape gibridnykh voin [Information security at the current stage of hybrid wars]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Issues of Russian and International Law], 14(10-1), 50–58. EDN: VBSJCE.
5. Gadzhiev, Kh.A. (2022). Tsifrovoe prostranstvo i politicheskaia stabil'nost' Rossii [Digital space and political stability of Russia]. *Sotsial'no-politicheskie nauki* [Socio-Political Sciences], 12(6), 22–28.
6. Kozaev, N.Sh. (2024). Kiberprestupnost' v sovremennom mire: tendentsii, vyzovy i strategii protivodeistviia [Cybercrime in the modern world: trends, challenges and counteraction strategies]. *Gumanitarnye, sotsial'no-ekonomicheskie i obshchestvennye nauki* [Humanitarian, Socio-Economic and Social Sciences], (11), 146–153.
7. Kobets, P.N. (2017). Vliianie globalizatsii i kiberprestupnosti na srashchivanie organizovannoi prestupnosti s radikal'nymi terroristicheskimi i nasil'stvennymi ekstremistskimi gruppami [The influence of globalization and

cybercrime on the merging of organized crime with radical terrorist and violent extremist groups]. *Matritsa nauchnogo poznaniia* [Matrix of Scientific Knowledge], (5), 45–47.

8. Kostarev, D.F., & Novikov, A.V. (2022). Sovershenstvovanie deiatel'nosti ispravitel'nykh uchrezhdenii ugolovno-ispolnitel'noi sistemy po obespecheniiu nadzora za litsami, otbyvaiushchimi nakazanie [Improving the activities of correctional institutions of the penal system in ensuring supervision of persons serving sentences]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Issues of Russian and International Law], 12(10-1), 616–624. https://doi.org/ 10.34670/ AR.2022.62.17.059
9. Ovchinnikov, S.N. (2025) Primenenie tsifrovykh tekhnologii v sfere ispolneniia ugolovnykh nakazanii: napravleniia, innovatsii, riski [Application of digital technologies in the field of execution of criminal penalties: directions, innovations, risks]. *Penitentsiarnaia nauka* [Penitentiary Science], 19(3(71)), 261–269. https://doi.org/10.46741/2686-9764.2025.71.3.004
10. *Operativno-rozysknaia deiatel'nost' v tsifrovom mire: sbornik nauchnykh trudov* [Operative-Search Activity in the Digital World: Collection of Scientific Works]. (2021). (V.S. Ovchinskii, Ed.). Moscow: INFRA-M.
11. Osipenko, A.L. (2017). Organizovannaia prestupnaia deiatel'nost' v kiberprostranstve: tendentsii i protivodeistvie [Organized criminal activity in cyberspace: trends and counteraction]. *Iuridicheskaia nauka i praktika: Vestnik Nizhegorodskoi akademii MVD Rossii* [Legal Science and Practice: Bulletin of the Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia], 4(40), 181–188. EDN: ZXRFTZ.
12. Serebrennikova, A.V. (2021). Tsifrovizatsiia ispolneniia nakazaniia: sostoianie i perspektivy [Digitalization of punishment execution: state and prospects]. *Chelovek: prestuplenie i nakazanie* [Man: Crime and Punishment], 29(1), 40–45.
13. Silant'eva, N.A. (2025) Tsifrovoi kontrol' v ugolovno-ispolnitel'noi sisteme: perspektivy i vyzovy vnedreniia novykh tekhnologii [Digital control in the penal system: prospects and challenges of implementing new technologies]. *Vestnik Prikamskogo sotsial'nogo instituta* [Bulletin of the Prikamsky Social Institute], 1(100), 53–62.
14. Slabkaia, D.N., & Novikov, A.V. (2022). K voprosu o klassifikatsii nakazanii, primeniaemykh v ugolovnom zakonodatel'stve Rossii [On the classification of punishments applied in the criminal legislation of Russia]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Issues of Russian and International Law], 12(7-1), 198–203. https://doi.org/10.34670/AR.2022.41.36.023 EDN: TMHHTM.
15. Sukhodolov, A.P., Ivantsov, S.V., & Molchanova, T.V. (2018). Tsifrovaia kriminologiia: matematicheskie metody prognozirovaniia [Digital criminology: mathematical forecasting methods]. *Vserossiiskii kriminologicheskii zhurnal* [All-Russian Criminology Journal], 12(2), 230–236.
16. Sostoianie prestupnosti v Rossiiskoi Federatsii za ianvar' - dekabr' 2024 goda [State of crime in the Russian Federation for January - December 2024]. (n.d.). Official website of the Ministry of Internal Affairs of the Russian Federation. Retrieved November 12, 2025, from https://xn--b1aew.xn--p1ai/reports/item/60248328
17. Smith, G.J.D. (2017). The challenges of doing criminology in the big data era: towards a digital and data-driven approach. *British Journal of Criminology*, 57(2), 259–274.