Дата поступления рукописи в редакцию: 07.06.2026 г.
Дата принятия рукописи в печать: 01.07.2026 г.
DOI: 10.24412/3034-2422-2026-3-29-34

МУХИН Роман Александрович,
студент,
Московский ордена Почета университет
МВД России им. В.Я. Кикотя,
e-mail: sima-zaitseva@yandex.ru

ЗАЙЦЕВА Серафима Евгеньевна,
кандидат педагогических наук, доцент,
доцент кафедры иностранных языков,
Московский ордена Почета университет
МВД России им. В.Я. Кикотя,
e-mail: sima-zaitseva@yandex.ru

К ВОПРОСУ О БОРЬБЕ С КИБЕРПРЕСТУПНОСТЬЮ В МИРОВОМ ПРОСТРАНСТВЕ: РОССИЙСКИЙ И ЗАРУБЕЖНЫЙ ОПЫТ

АННОТАЦИЯ. В статье проведён сравнительный анализ систем противодействия киберпреступности в России и США, а также разработка рекомендаций по совершенствованию мер противодействия киберугрозам. Актуальность темы обусловлена тем, что киберпреступления представляют угрозу не только для общественной, но и национальной безопасности государств. Практическая значимость исследования состоит в том, что его результаты могут быть использованы для совершенствования законодательства и практики противодействия киберпреступности в России и США, а также для развития международного сотрудничества в этой сфере.

КЛЮЧЕВЫЕ СЛОВА: киберпреступность, кибербезопасность, законодательные акты, аспекты информационной безопасности, правовое регулирование, проблемы в противодействии киберпреступности, перспективные направления сотрудничества.

MUKHIN Roman Alexandrovich,
Student,
Moscow University of the Order of Honor
The Ministry of Internal Affairs of Russia named after V.Ya. Kikot

ZAITSEVA Serafima Evgenevna,
PhD, Associate Professor,
Associate Professor of the Department of Foreign Languages,
Moscow University of the Order of Honor
The Ministry of Internal Affairs of Russia named after V.Ya. Kikot

ON THE ISSUE OF COMBATING CYBERCRIME IN THE GLOBAL SPACE: RUSSIAN AND FOREIGN EXPERIENCE

ANNOTATION. The article provides a comparative analysis of cybercrime counteraction systems in Russia and the United States, as well as the development of recommendations for improving measures to counter cyber threats. The relevance of the topic is due to the fact that cybercrimes pose a threat not only to the public, but also to the national security of states. The practical significance of the research lies in the fact that its results can be used to improve legislation and practice in countering cybercrime in Russia and the United States, as well as to develop international cooperation in this area. .

KEY WORDS: cybercrime, cybersecurity, legislative acts, aspects of information security, legal regulation, problems in countering cybercrime, promising areas of cooperation.

Введение

Глобальная цифровизация и стремительное развитие информационно-коммуникационных технологий в XXI веке привели к формированию принципиально новой киберпространственной среды, которая стала не только инструментом экономического и социального прогресса, но и ареной для совершения противоправных деяний. Киберпреступность представляет собой одну из наиболее серьезных угроз для национальной и международной безопасности, экономического развития и прав граждан. Транснациональный характер этого явления кардинально усложняет борьбу с ним, поскольку современные кибер-

преступники координируют действия из разных юрисдикций, используют инфраструктуру в нескольких странах одновременно и наносят ущерб жертвам по всему миру. Международные усилия по борьбе с этим явлением можно проанализировать, проведя сравнительные исследования подходов к противодействию киберпреступности в таких технологически развитых и геополитически значимых державах, как Российская Федерация и Соединенные Штаты Америки, которые, согласно Всемирному индексу киберпреступности, входят в число ключевых источников киберугроз и одновременно являются наиболее привлекательными мишенями для кибератак [2].

Законодательная база России в сфере противодействия киберпреступности

Политико-правовой контекст современных международных отношений между Россией и США добавляет дополнительную сложность в вопросы кибербезопасности. С одной стороны, существует очевидная необходимость сотрудничества в борьбе с общими угрозами, с другой - сохраняются существенные различия в подходах к регулированию интернета, защите персональных данных и обеспечению национального цифрового суверенитета. Эти противоречия находят непосредственное отражение в формировании национальных стратегий противодействия киберпреступности (рис. 1).

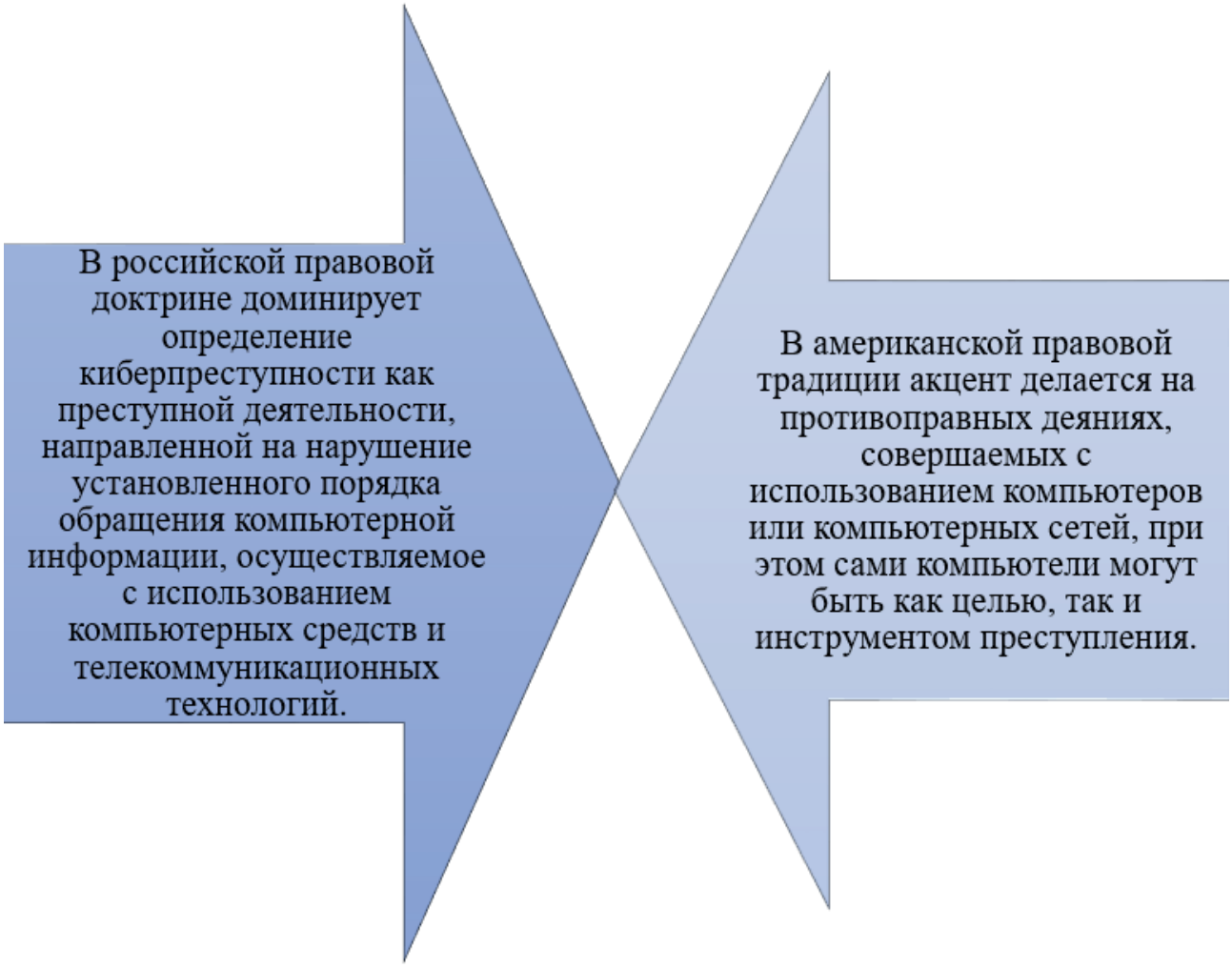

Рисунок 1. Сравнение российской и американской правовых доктрин

Российская Федерация сформировала разветвленную нормативно-правовую базу для противодействия киберпреступности, которая продолжает активно развиваться. Кроме того, в России сформирована многоуровневая институциональная система органов, ответственных за противодействие киберпреступности.

Анализ законодательной базы США

Соединенные Штаты Америки имеют более длительную историю правового регулирования в сфере киберпреступности, что обусловлено более ранним развитием компьютерных технологий и интернета [5, с. 1-20] (рис. 2).

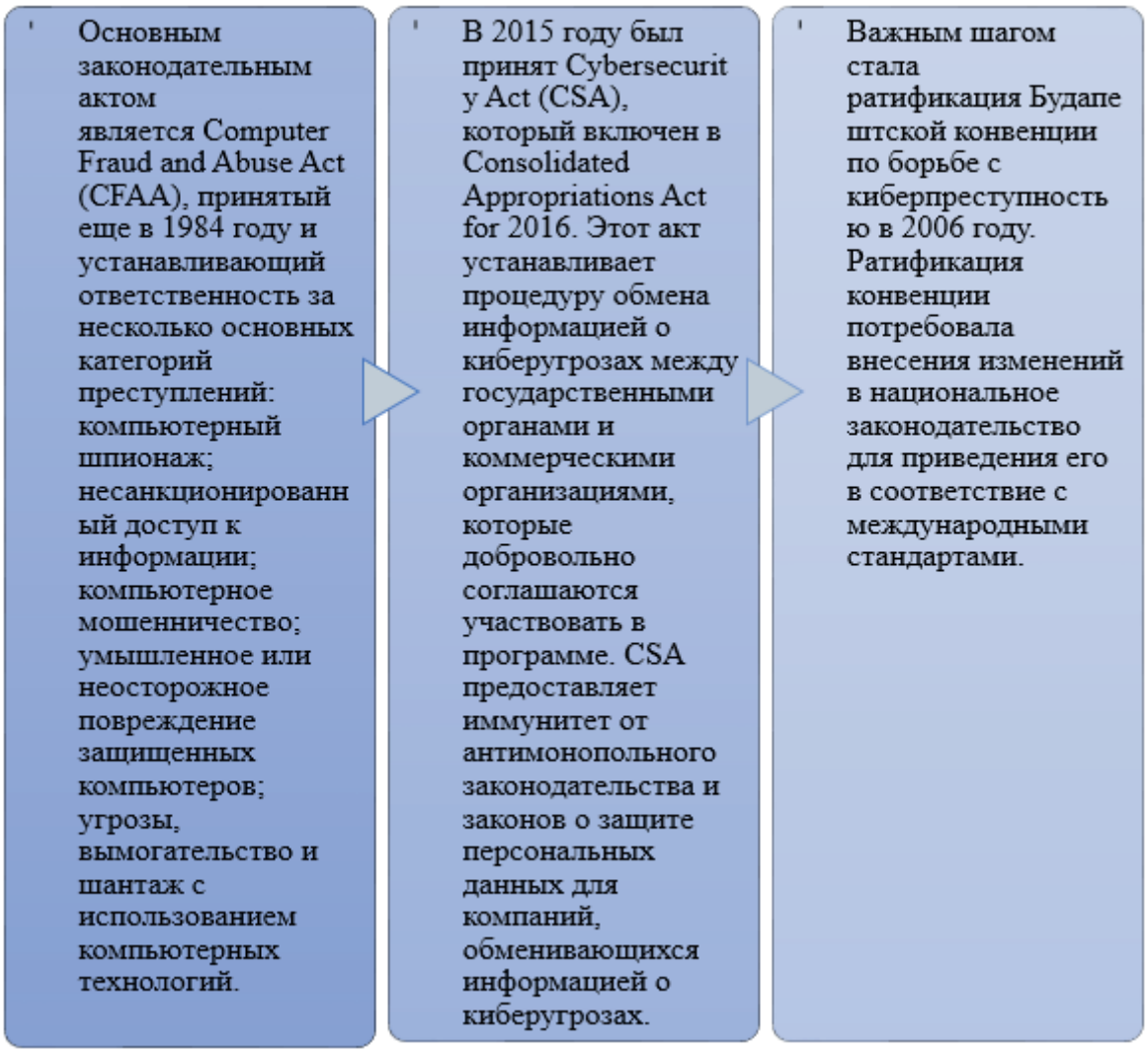

Рисунок 2. Основные законодательные акты США

Среди других важных законодательных актов США в сфере кибербезопасности следует отметить (рис. 3).

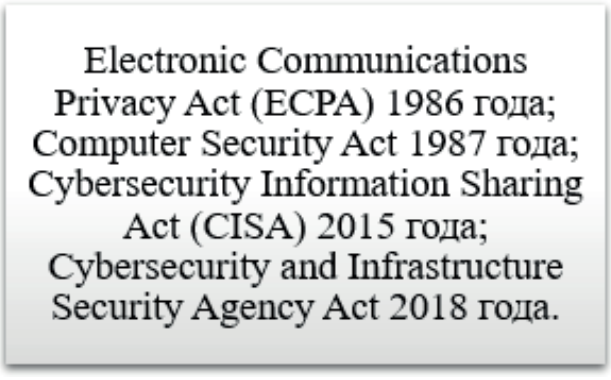

Рисунок 3. Перечень актов США в сфере кибербезопасности

Кроме того, в США создана разветвленная система органов, отвечающих за борьбу с киберпреступностью, которая характеризуется распределением полномочий между различными ведомствами. Кроме ФБР, значительную роль в борьбе с киберпреступностью играют и другие министерства и службы, отвечающие за различные аспекты кибербезопасности [3, с. 198-201].

Сравнительный анализ законодательных подходов

Международный характер киберпреступности создает вызовы для правоприменительной деятельности. Преступники используют свободу перемещения товаров, услуг, данных и капитала через Интернет, что требует международного сотрудничества. Хотя США ратифицировали Буда-

пештскую конвенцию и поддерживают процессы международной гармонизации законодательства, остается проблема эффективной координации с партнерами из разных юрисдикций.

В США одной из основных проблем является сложность законодательного процесса и политическая поляризация, которая затрудняет принятие необходимых нормативных актов. Как отмечается в исследованиях, на каждой сессии Конгресса представляется несколько законопроектов в области кибербезопасности, но лишь немногие из них получают поддержку обеих фракций и становятся законами [4, с. 1-32].

Проведенный анализ законодательных систем России и США позволяет выявить существенные различия в подходах к правовому регулированию борьбы с киберпреступностью (рис. 4).

Рисунок 4. Сравнительная характеристика институциональных систем противодействия киберпреступности

Хронологическое различие проявляется в том, что США начали формировать законодательную базу значительно раньше - первые специализированные законы были приняты в 1980-х годах, тогда как в России активное законотворчество в этой сфере началось только в 2000-х годах.

Концептуальное различие заключается в том, что американское законодательство делает акцент на защите информационных систем и сетей, тогда как российское законодательство акцентирует внимание на защите информации как объекта правовых отношений.

Структурное различие состоит в том, что в США существует множество специализированных законов, регулирующих отдельные аспекты кибербезопасности, тогда как в России преобладает модель нескольких рамочных законов, которые затем конкретизируются подзаконными актами.

Международно-правовое различие проявляется в отношении к международным договорам: США являются участником Будапештской конвенции, тогда как Россия не участвует в этом соглашении и развивает альтернативные международные инициативы.

Проведенный анализ позволяет выявить как общие, так и специфические проблемы в противодействии киберпреступности в России и США [1, с. 287-292] (рис. 5).

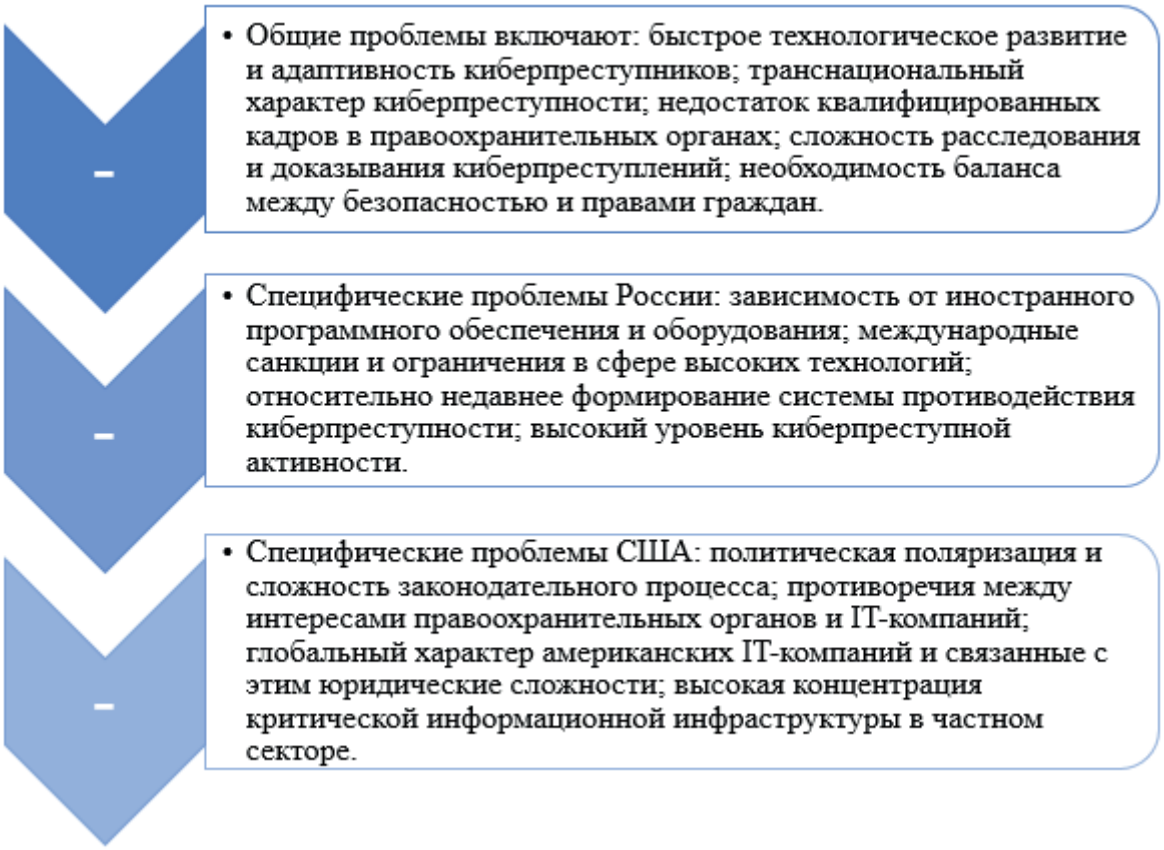

Рисунок 5. Проблемы в противодействии киберпреступности в РФ и США

Заключение

На основе проведенного анализа можно выделить общие перспективные направления совершенствования борьбы с киберпреступностью в России и США.

• Разработка международных стандартов и норм поведения в киберпространстве;

• Создание эффективных механизмов быстрого реагирования на киберинциденты;

• Развитие технологий искусственного интеллекта для прогнозирования и предотвращения кибератак;

• Укрепление доверия и сотрудничества между Россией и США в сфере кибербезопасности, несмотря на политические разногласия.

Проведенное комплексное исследование проблем противодействия киберпреступности в России и США позволило выявить многоаспектную природу данного явления и сформировать системное понимание современных вызовов в области кибербезопасности. Сравнительный анализ двух различных подходов к регулированию цифрового пространства продемонстрировал как общие тенденции развития киберпреступности, так и специфические национальные особенности борьбы с ней.

Исследование выявило, что киберпреступность продолжает динамично эволюционировать, адаптируясь к технологическим изменениям и мерам противодействия.

На основе проведенного анализа можно отметить, что несмотря на политические разногласия, Россия и США имеют общую заинтересованность в борьбе с транснациональной киберпреступностью. Перспективными направлениями сотрудничества могли бы стать:

- создание механизмов оперативного взаимодействия для противодействия наиболее опасным киберугрозам:

- разработка общих стандартов и протоколов в области кибербезопасности;

- совместные исследования и разработки в области технологий кибербезопасности;

- обмен лучшими практиками в области законодательного регулирования и правоохранительной деятельности.

Список литературы:

[1] Кодзокова Л.А. Проблемы противодействия киберпреступности в Российской Федерации // Пробелы в российском законодательстве. — 16(4), 2023. — С. 287-292.

[2] Федотов А.В. Киберпреступность и кибербезопасность в современном мире. — М. : Юрайт, 2022. — 384 с.

[3] Сулаймонова Ю.И. Актуальные проблемы борьбы с преступностью в сфере информационных

технологий в США // Современные тенденции развития цифровизации в сфере юстиции. — 1(1), 2022. — С. 198-201.

[4] Anderson R., et al. Measuring the Changing Cost of Cybercrime // Workshop on the Economics of Information Security. — 2019. — С. 1-32.

[5] Clayton R., et al. Cybercrime is (often) boring: maintaining the infrastructure of cybercrime economies // Workshop on the Economics of Information Security. — 2020. — С. 1-20.

[6] World-first «Cybercrime Index» ranks countries by cybercrime threat level // University of Oxford. URL: https://www.ox.ac.uk/news/2024-04-10-world-first-cybercrime-index-ranks-countries-cybercrime-threat-level (дата обращения: 11.02.2026).

[7] Cybersecurity Threat Trends // FBI Internet Crime Complaint Center. 2024. URL: https://www.ic3.gov/Home/AnnualReports (дата обращения: 11.02.2026).

References:

[1] Kodzokova L.A. Problems of Combating Cybercrime in the Russian Federation // Gaps in Russian Legislation. - 16 (4), 2023. - Pp. 287-292.

[2] Fedotov A.V. Cybercrime and Cybersecurity in the Modern World. - Moscow: Yurait, 2022. - 384 p.

[3] Sulaimonova Yu.I. Actual Problems of Combating Crime in the Sphere of Information Technology in the USA // Modern Trends in the Development of Digitalization in the Sphere of Justice. - 1 (1), 2022. - Pp. 198-201.

[4] Anderson R., et al. Measuring the Changing Cost of Cybercrime // Workshop on the Economics of Information Security. - 2019. - Pp. 1-32.

[5] Clayton R., et al. Cybercrime is (often) boring: maintaining the infrastructure of cybercrime economies // Workshop on the Economics of Information Security. - 2020. - P. 1-20.

[6] World-first «Cybercrime Index» ranks countries by cybercrime threat level // University of Oxford. URL: https://www.ox.ac.uk/news/2024-04-10-world-first-cybercrime-index-ranks-countries-cybercrime-threat-level (accessed 02/11/2026).

[7] Cybersecurity Threat Trends // FBI Internet Crime Complaint Center. 2024. URL: https://www.ic3.gov/Home/AnnualReports (accessed 02/11/2026).