Научная статья
https://doi.org/10.24412/2220-2404-2024-11-9
УДК 339.564

КИБЕРПРЕСТУПНОСТЬ В СОВРЕМЕННОМ МИРЕ: ТЕНДЕНЦИИ, ВЫЗОВЫ И СТРАТЕГИИ ПРОТИВОДЕЙСТВИЯ

Козаев Н.Ш.
Ставропольский филиал Краснодарского университета
Министерства внутренних дел Российской Федерации

Аннотация. *В статье проводится комплексный анализ феномена киберпреступности как одного из ключевых вызовов современного общества. Рассматривается эволюция и текущее состояние киберпреступности, ее основные виды и особенности. Особое внимание уделяется проблемам выявления, расследования и предупреждения киберпреступлений, а также низкой раскрываемости данного вида преступлений. Анализируются вопросы совершенствования правового регулирования в сфере противодействия киберпреступности, включая необходимость адаптации уголовного и уголовно-процессуального законодательства. Подчеркивается важность международного сотрудничества в борьбе с транснациональной киберпреступностью и рассматриваются существующие механизмы такого взаимодействия. Отдельно освещаются перспективы и этические аспекты использования искусственного интеллекта в противодействии киберпреступлениям. На основе проведенного анализа предлагается комплекс мер, направленных на повышение эффективности профилактики и противодействия киберпреступности, включая совершенствование законодательства, усиление международного сотрудничества, повышение квалификации специалистов и развитие технологий кибербезопасности.*

Ключевые слова: *киберпреступность, информационная безопасность, киберпространство, правовое регулирование, международное сотрудничество, искусственный интеллект, профилактика преступлений.*

CYBERCRIME IN THE MODERN WORLD: TRENDS, CHALLENGES AND COUNTERACTION STRATEGIES

Nodar Sh. Kozaev
Stavropol branch of the Krasnodar University of the Ministry of Internal Affairs of the Russian Federation

Abstract*. The article provides a comprehensive analysis of the cybercrime phenomenon as one of the key challenges facing modern society. It examines the evolution and current state of cybercrime, its main types and characteristics. Particular attention is paid to the problems of detection, investigation, and prevention of cybercrimes, as well as the low clearance rate for this type of crime. The paper analyzes issues of improving legal regulation in the field of combating cybercrime, including the need to adapt criminal and criminal procedure legislation. The importance of international cooperation in the fight against transnational cybercrime is emphasized, and existing mechanisms for such interaction are examined. The prospects and ethical aspects of using artificial intelligence in countering cybercrimes are separately highlighted. Based on the analysis, a set of measures aimed at increasing the effectiveness of prevention and counteraction to cybercrime is proposed, including improving legislation, strengthening international cooperation, enhancing the qualifications of specialists, and developing cybersecurity technologies.*

Keywords: *cybercrime, information security, cyberspace, legal regulation, international cooperation, artificial intelligence, crime prevention.*

Введение. *Актуальность* исследования обусловлена стремительным ростом киберпреступности, которая в последние годы стала одним из ключевых вызовов для современного общества и правоохранительной системы. Статистические данные демонстрируют устойчивую тенденцию к увеличению доли киберпреступлений в общей структуре преступности, что свидетельствует о смещении криминальной активности в цифровую среду. Проблема заключается в многообразии видов киберпреступлений, их транснациональном характере и низкой раскрываемости, что создает

серьезные трудности для правоохранительных органов. Особую озабоченность вызывает рост числа тяжких и особо тяжких преступлений в киберпространстве, а также использование киберпреступниками передовых технологий для совершения противоправных деяний.

Предметом исследования выступает киберпреступность как комплексное социально-правовое явление и меры противодействия ей на национальном и международном уровнях.

Цель работы заключается в проведении всестороннего анализа современного состояния киберпреступности и разработке научно обоснованных рекомендаций по совершенствованию мер противодействия.

Задачи исследования включают детальное изучение видов киберпреступлений и их особенностей, анализ проблем в сфере правового регулирования и правоприменительной практики, рассмотрение перспектив международного сотрудничества в борьбе с киберпреступностью, а также оценку возможностей и рисков использования искусственного интеллекта в противодействии данному виду преступности.

Методология исследования основана на комплексном системном подходе, включающем анализ статистических данных о состоянии киберпреступности, изучение нормативно-правовых актов национального и международного уровня, а также обзор научной литературы по проблематике исследования. В работе использованы методы сравнительного правоведения, статистического анализа и прогнозирования.

Обсуждение.

Киберпреступность представляет собой новое и динамично развивающееся явление, связанное с использованием информационно-коммуникационных технологий (ИКТ) для совершения противоправных деяний.

Сущность киберпреступности обусловлена возможностями компьютера и компьютерных сетей, которые создают принципиально новую среду для криминальной активности – киберпространство.

Понятие «киберпространство» происходит от научного термина «кибернетика», предложенного американским математиком Норбертом Винером в 1948 г. Согласно ГОСТ IEC 60050-732-2017, киберпространство определяется как «виртуальное пространство, создаваемое компьютерной сетью с рядом распределенных приложений и их пользователями» [2, с. 13].

Таким образом, киберпространство представляет собой особую виртуальную среду, порожденную развитием информационных технологий.

Киберпреступность в современном мире превратилась в устойчивую форму криминального бизнеса, приносящую огромные доходы и наносящую колоссальный ущерб экономике, безопасности и технологическому развитию как развитых, так и развивающихся стран.

По мере того, как организации все больше полагаются на цифровизацию и информационно-коммуникационные технологии, вероятность стать жертвой киберпреступлений неуклонно возрастает. Особенно ярко эта тенденция проявилась в период пандемии COVID-19, когда массовый переход на удаленную работу создал благоприятные условия для беспрецедентного роста киберпреступности, вызвавшей хаотичные нарушения в деятельности государств, бизнеса и отдельных граждан.

Исследователи отмечают, что киберпреступность эволюционирует от простых злонамеренных инцидентов к сложным кибератакам, которые поддерживаются и направляются государствами или организованными хакерскими группировками [9].

Киберпреступность стала устойчивой бизнес-практикой для злоумышленников, поскольку она является прибыльной, легкой в реализации и имеет низкую вероятность быть пойманным.

Критической проблемой остается отсутствие инструментов для точного расчета масштабов и воздействия киберпреступности, сопоставимых с методами оценки традиционных преступлений. Ситуация усугубляется тем, что киберпреступники активно используют возможности цифровизации, такие как социальные сети, форумы, чат-каналы и даркнет, для обмена идеями, практиками и методами.

Результаты.

Сущностной характеристикой киберпреступности является то, что она не ограничена географическими рамками и может осуществляться дистанционно из любой точки мира, а трансграничный характер создает дополнительные сложности для их расследования и пресечения.

Рост масштабов и усложнение форм киберпреступности в России представляет собой одну из ключевых проблем, с которой сталкиваются правоохранительные органы и общество в целом. Анализ статистических данных демонстрирует устойчивую тенденцию к увеличению числа киберпреступлений в общей структуре пре-

ступности. Если в 2016 году доля киберпреступлений составляла лишь 4,2% от общего числа зарегистрированных преступлений, то к 2023 году она выросла до 34,8%, увеличившись в 8 раз. В абсолютных цифрах количество зарегистрированных киберпреступлений в России в 2023 году достигло 677 тыс., что на 29,7% больше, чем в предыдущем году [4, с. 107].

Таким образом, после некоторой стабилизации количества выявленных киберпреступлений в 2022 году, связанной, в том числе с началом специальной военной операции, в 2023 году наблюдается новый рост этого показателя, что свидетельствует о высокой адаптивности киберпреступников к изменяющимся условиям и их способности быстро восстанавливать свою деятельность.

Симптоматично и то, что и материальный ущерб от киберпреступлений продолжает расти. В 2023 году он составил более 156 миллиардов рублей, что на 70% больше, чем в предыдущем году [7, с. 98-103].

Структура киберпреступности в России характеризуется преобладанием мошенничеств, совершаемых с использованием информационно-телекоммуникационных технологий. В 2023 году их доля составила 52,18% от общего числа киберпреступлений, что демонстрирует рост по сравнению с предыдущими годами. На втором месте по распространенности находятся кражи, совершаемые с использованием IT-технологий, хотя их доля в общей структуре киберпреступности снижается.

Особую озабоченность вызывает рост числа киберпреступлений, связанных с незаконным оборотом наркотических средств. В 2023 году их количество значительно увеличилось, что может свидетельствовать об активном использовании информационных технологий в наркобизнесе. Более половины (50,6%) киберпреступлений относятся к категориям тяжких и особо тяжких. Это свидетельствует о повышении общественной опасности данного вида преступной деятельности. Кроме того, наблюдается расширение спектра используемых киберпреступниками технологий и методов. Так, 77,8% киберпреступлений совершаются с использованием сети Интернет, а 44,7% – применением средств мобильной связи [4, с. 106-112].

Усложнение форм киберпреступности проявляется в появлении новых видов противоправных деяний, таких как атаки с использованием искусственного интеллекта, квантового шифрования, создание дипфейков.

Киберпреступники все чаще прибегают к использованию сложных технологических решений, включая облачные сервисы для хранения и распространения похищенных данных. По данным исследований, количество так называемых «облаков логов», используемых злоумышленниками, выросло в три раза за последний год.

Важно отметить, что рост киберпреступности происходит на фоне общего снижения уровня традиционной преступности, что указывает на смещение криминальной активности в цифровую среду и создает новые вызовы для правоохранительной системы. Прогнозируется, что в ближайшие годы доля киберпреступлений в общей структуре преступности продолжит расти и может превысить 40% в 2024 году. Такая динамика требует адекватного ответа со стороны государства и общества.

Виды киберпреступлений и их особенности представляют собой сложную и постоянно эволюционирующую научную категорию. Киберпреступления характеризуются использованием информационно-коммуникационных технологий как для совершения традиционных видов преступлений, так и для осуществления новых форм противоправной деятельности, которые стали возможны только с развитием цифровых технологий.

Одним из наиболее распространенных видов киберпреступлений является финансовое мошенничество, которое может включать в себя фишинг (попытки получить конфиденциальную информацию путем обмана), скимминг (кража данных банковских карт), а также различные схемы онлайн-мошенничества. Особенностью таких преступлений является их массовость и относительная простота реализации, поскольку злоумышленники могут одновременно атаковать тысячи потенциальных жертв, используя автоматизированные инструменты.

Другой значимой категорией являются преступления, связанные с нарушением конфиденциальности и целостности данных. Сюда можно отнести несанкционированный доступ к компьютерным системам (хакерство), распространение вредоносного программного обеспечения (вирусов, троянов, программ-вымогателей), а также кражу и незаконное использование персональных данных. Особенностью, данной категории преступлений является их потенциально огромный масштаб воздействия – взлом одной корпоративной сети может привести к утечке данных миллионов пользователей.

Отдельно стоит выделить киберпреступления, направленные против детей и подростков, куда можно отнести различные формы сексуальной эксплуатации несовершеннолетних в Интернете, кибербуллинг (травля в сети), а также вовлечение детей в деструктивные сообщества, пропагандирующие суицид или экстремизм. Особенностью этих преступлений является их высокая общественная опасность и тяжесть последствий для психики и развития несовершеннолетних [3, с. 73-77].

В последние годы все большую актуальность приобретают киберпреступления, направленные против критической инфраструктуры государств. Сюда относятся атаки на энергетические системы, транспортные сети, системы водоснабжения и другие ключевые объекты. Особенностью таких преступлений является их потенциально катастрофические последствия для жизнеобеспечения целых регионов и стран.

Еще одной важной категорией являются киберпреступления, связанные с нарушением авторских прав и интеллектуальной собственности, которые включает в себя незаконное распространение, защищенного авторским правом, контента (фильмов, музыки, программного обеспечения), а также промышленный шпионаж с использованием компьютерных технологий. Особенностью данных преступлений является сложность их выявления и доказывания, а также значительный экономический ущерб для правообладателей.

Отдельно также стоит упомянуть о таком явлении как киберэкстремизм и кибертерроризм, то есть использование интернет-технологий для пропаганды экстремистских идеологий, вербовки новых членов террористических организаций, а также планирования и координации террористических актов. Особенностью этих преступлений является их высокая общественная опасность и сложность противодействия им вследствие использования преступниками технологий шифрования и анонимизации.

Таким образом, киберпреступность представляет собой сложное и многогранное явление, характеризующееся широким спектром видов противоправной деятельности, высокой адаптивностью преступников к новым условиям, а также значительными трудностями в выявлении и расследовании таких преступлений.

Противодействие киберпреступности сталкивается с целым рядом серьезных проблем, обусловленных как спецификой данного вида преступлений, так и особенностями правового регулирования и правоприменительной практики в этой сфере.

Одной из ключевых проблем в противодействии киберпреступности остается низкий уровень раскрываемости. В 2023 году было раскрыто лишь 26,6% зарегистрированных киберпреступлений, что хотя и демонстрирует некоторый рост по сравнению с предыдущими годами, но все еще остается на недопустимо низком уровне. Во многом это связано с высокой латентностью киберпреступлений, которая искажает реальную картину криминогенной обстановки. По целому ряду обстоятельств объективного и субъективного характера значительная часть таких преступлений остается невыявленной или незарегистрированной [6, с. 96-105].

Среди объективных обстоятельств можно назвать сложность выявления самого факта совершения преступления в киберпространстве (вследствие высокой степени анонимности и географической удаленности исполнителей), недостаточную техническую оснащенность правоохранительных органов для мониторинга киберугроз, а также отсутствие специализированных подразделений по борьбе с киберпреступностью в ряде регионов.

Среди обстоятельств субъективного характера можно отметить тот факт, что многие жертвы не сообщают о совершенных против них преступлениях в правоохранительные органы. Причинами такого поведения у физических лиц могут выступать чувство стыда или смущения от того, что человек стал жертвой обмана, недоверие к правоохранительной системе в целом и скептицизм в отношении эффективности расследования киберпреступлений и возможности возмещения ущерба, в частности, нежелание нести временные и ресурсные затраты, а также опасения того, что в ходе расследования может быть раскрыта конфиденциальная информация. Организации, в свою очередь, стремятся избежать репутационных (например, потери доверия клиентов) и финансовых (например, снижения стоимости акций) потерь, вследствие чего избегают публичного раскрытия информации о киберинцидентах.

Полагаем, что частичному решению данных проблем будет способствовать создание единого центра приема и обработки заявлений о киберпреступлениях, аналогичного Центру приема жалоб на мошенничество в Интернете (IC3) при ФБР США, проведение информационных кампаний, направленных на повышение осведомленности граждан о необходимости сообщать о киберпреступлениях, а также упрощение процедуры

подачи заявлений о киберпреступлениях, в том числе через онлайн-сервисы.

Недостаточная эффективность правового регулирования и правоприменительной практики в сфере противодействия киберпреступности является одним из основных факторов, затрудняющих борьбу с этим видом преступности в России. Существующая нормативно-правовая база не в полной мере соответствует динамично меняющейся природе киберпреступлений, что создает пробелы в законодательстве и затрудняет привлечение виновных к ответственности.

Одной из проблем является отсутствие единого подхода к определению и классификации киберпреступлений в российском законодательстве. В настоящее время Уголовный кодекс РФ содержит ряд статей, предусматривающих ответственность за преступления в сфере компьютерной информации (глава 28 УК РФ), однако, этого недостаточно для охвата всего спектра противоправных деяний, совершаемых с использованием информационно-телекоммуникационных технологий.

Необходимо рассмотреть возможность введения в Уголовный кодекс РФ отдельной главы, посвященной киберпреступлениям, которая бы включала в себя как уже существующие составы преступлений, так и новые, отражающие современные реалии цифровой преступности. Такой подход позволил бы систематизировать нормы, касающиеся ответственности за киберпреступления, и облегчить их применение на практике.

Кроме того, требуется уточнение и расширение понятийного аппарата в сфере киберпреступности. В частности, целесообразно законодательно закрепить определения таких понятий, как «киберпреступление», «киберпространство» и др. Это поможет избежать неоднозначности в толковании норм и повысит эффективность их применения.

Отдельного внимания заслуживает проблема квалификации киберпреступлений. Сложность и многообразие форм киберпреступной деятельности часто приводят к трудностям при определении состава преступления и выборе соответствующей статьи Уголовного кодекса РФ.

В связи с этим, необходимо разработать детальные методические рекомендации для правоохранительных органов по квалификации различных видов киберпреступлений.

Важным аспектом совершенствования правового регулирования в данной сфере также является адаптация процессуального законодательства к особенностям расследования киберпреступлений, в связи с чем, требуется внесение изменений в Уголовно-процессуальный кодекс РФ, которые бы учитывали специфику сбора и анализа цифровых доказательств, а также особенности проведения следственных действий в киберпространстве.

1. Международное сотрудничество в борьбе с киберпреступностью является ключевым аспектом эффективного противодействия данному виду преступной деятельности. Как уже отмечалось, киберпреступность по своей природе носит транснациональный характер, что создает значительные трудности для правоохранительных органов отдельных государств. Преступники могут находиться в одной стране, использовать серверы в другой, а жертвы могут быть расположены в третьей стране [1, с. 135–137]. Такая ситуация требует тесной координации и взаимодействия правоохранительных органов разных стран.

Одним из важнейших шагов в направлении международного сотрудничества стало принятие в 2001 году Конвенции о киберпреступности (Будапештской конвенции). Данный документ стал первым международным договором, направленным на борьбу с преступлениями в киберпространстве путем гармонизации национальных законодательств, совершенствования методов расследования и расширения международного сотрудничества. Конвенция определяет основные виды киберпреступлений и устанавливает процедуры международного взаимодействия при их расследовании. Однако не все страны присоединились к данной Конвенции. Например, Россия не является ее участником, аргументируя это тем, что некоторые положения документа могут нарушать суверенитет государства. Тем не менее, Россия активно участвует в других форматах международного сотрудничества в данной сфере.

Важную роль в координации усилий по борьбе с киберпреступностью играют международные организации. Интерпол имеет специальное подразделение по борьбе с киберпреступностью, которое оказывает поддержку странам-членам в расследовании киберпреступлений и обмене информацией. Европол также активно работает в этом направлении, в частности, через Европейский центр по борьбе с киберпреступностью (EC3).

Одной из ключевых проблем международного сотрудничества является различие в национальных законодательствах разных стран. То, что считается преступлением в одной стране, может

быть легальным в другой. Сложившаяся ситуация создает «безопасные гавани» для киберпреступников и затрудняет их преследование. Поэтому важным направлением международного сотрудничества является гармонизация законодательств разных стран в сфере борьбы с киберпреступностью.

Другой проблемой является сложность и длительность процедур международной правовой помощи. Традиционные механизмы взаимодействия правоохранительных органов разных стран часто оказываются слишком медленными для эффективного реагирования на киберпреступления, где счет может идти на минуты. Поэтому разрабатываются новые, более оперативные механизмы взаимодействия, в том числе с использованием современных технологий.

Кроме того, международное сотрудничество должно учитывать различия в технологических возможностях и ресурсах разных стран. Развивающиеся страны часто не имеют всеобъемлющего законодательства о киберпреступности и необходимой инфраструктуры для эффективного расследования и судебного преследования киберпреступлений. Поэтому международное сотрудничество должно включать в себя значительный компонент наращивания потенциала, направленный на повышение возможностей этих стран в области борьбы с киберпреступностью.

При этом наращивание потенциала также должно выходить за рамки правоохранительных органов и охватывать более широкий круг заинтересованных сторон. Оно должно включать в себя повышение осведомленности общественности о киберугрозах и профилактических мерах, обучение сотрудников частного сектора методам кибербезопасности и содействие развитию местной экосистемы кибербезопасности, включая исследования и инновации.

Отдельного внимания заслуживает вопрос предупреждения вовлечения молодежи в киберпреступную деятельность. Как показывает практика, значительная часть киберпреступлений совершается молодыми людьми, обладающими высоким уровнем компьютерной грамотности, но недостаточно развитым правосознанием [8, с. 37-41]. В этой связи, необходимо важным предупредительным эффектом является совершенствование системы выявления и блокировки вредоносного контента в сети Интернет. В настоящее время в России действует система блокировки противоправной информации, однако ее эффективность вызывает вопросы. Необходимо развивать технологии автоматизированного выявления и блокировки фишинговых сайтов, ресурсов, распространяющих вредоносное программное обеспечение. При этом безусловно важно соблюдать баланс между обеспечением безопасности и сохранением свободы распространения информации в сети. Также, важно усилить профилактическую работу в образовательных учреждениях, разъяснять молодежи правовые последствия совершения киберпреступлений.

Целесообразно также развивать программы позитивной занятости для талантливых в IT-сфере молодых людей, создавая условия для их самореализации в легальной деятельности.

Еще одним важным направлением совершенствования профилактики киберпреступности является усиление защищенности информационных систем и ресурсов. Это касается как государственных информационных систем, так и ресурсов коммерческих организаций, особенно в финансовом секторе.

В связи с этим, необходимо на законодательном уровне ужесточить требования к обеспечению кибербезопасности для организаций, работающих с персональными данными граждан и финансовой информацией.

Важным направлением совершенствования мер предупреждения киберпреступности здесь может выступить развитие государственно-частного партнерства. Необходимо наладить эффективный обмен информацией между правоохранительными органами и частными компаниями, работающими в сфере информационной безопасности, что позволит оперативно выявлять новые киберугрозы и вырабатывать меры противодействия им.

Целесообразно также стимулировать разработку отечественных средств защиты информации, поддерживать перспективные стартапы в сфере кибербезопасности.

Использование искусственного интеллекта (ИИ) в противодействии киберпреступности представляют собой одно из наиболее перспективных и одновременно сложных направлений, требующее тщательного правового регулирования и соблюдения баланса между эффективностью борьбы с преступностью и защитой прав и свобод граждан. С одной стороны, системы, основанные на искусственном интеллекте, могут прогнозировать вероятность совершения преступлений конкретными лицами или в определенных районах, однако с другой – использование таких прогнозов может привести к дискриминации и нарушению презумпции невиновности.

Важной этической проблемой использования ИИ в данной сфере является обеспечение прозрачности и подотчетности при использовании технологий в правоохранительной деятельности. Алгоритмы ИИ часто работают как «черный ящик», что затрудняет понимание процесса принятия решений, что особенно проблематично в контексте уголовного правосудия, где каждое решение должно быть обоснованным и понятным. Кроме того, использование ИИ, например, систем распознавания лиц и других биометрических данных для идентификации потенциальных преступников, поднимает вопросы о праве на анонимность и защите персональных данных. Аналогичные проблемы возникают при использовании технологий для мониторинга онлайн-активности граждан [5, с. 345-352].

Для эффективного и этичного использования ИИ в противодействии киберпреступности необходимо разработать подход, включающий следующие меры:

1.Развитие этических принципов использования ИИ. Необходимо разработать и внедрить этические кодексы и руководства по применению ИИ в правоохранительной деятельности. Руководящие принципы должны обеспечивать баланс между эффективностью борьбы с преступностью и защитой прав и свобод граждан.

2.Повышение квалификации специалистов. Требуется организовать систематическую подготовку сотрудников правоохранительных органов по вопросам использования ИИ в борьбе с киберпреступностью. Такая подготовка должно включать не только технические аспекты, но также этические и правовые вопросы применения ИИ. Необходимость повышения квалификации специалистов в сфере информационной безопасности является одной из ключевых задач в контексте противодействия киберпреступности в целом.

3.Развитие механизмов общественного контроля. Необходимо обеспечить прозрачность и подотчетность в использовании ИИ правоохранительными органами, что может включать создание независимых экспертных комиссий для оценки алгоритмов и систем ИИ, используемых в борьбе с киберпреступностью.

4.В контексте совершенствования отечественного законодательства можно предложить следующие меры:

- Внесение изменений в Федеральный закон «О полиции» и другие профильные законы, определяющие правовые основы использования ИИ в правоохранительной деятельности.
- Внесение дополнений в Уголовно-процессуальный кодекс РФ, определяющих статус и порядок использования данных, полученных с помощью систем ИИ, в качестве доказательств в уголовном процессе.
- Создание специализированного органа или расширение полномочий существующих структур (например, Научного совета при Совете Безопасности РФ) в части координации разработки и внедрения технологий ИИ в сфере противодействия киберпреступности.

Заключение.

Подводя итог нашему исследованию, необходимо отметить, что киберпреступность представляет собой динамично развивающееся явление, ставшее одним из ключевых вызовов для современного общества и правоохранительной системы. Многообразие видов киберпреступлений, включающих финансовое мошенничество, нарушение конфиденциальности данных, преступления против несовершеннолетних и атаки на критическую инфраструктуру, создает серьезные проблемы в работе правоохранительных органов.

Для повышения эффективности противодействия киберпреступности необходимо совершенствование нормативно-правовой базы, включая введение специализированной главы в Уголовный кодекс РФ, посвященной киберпреступлениям, и адаптацию процессуального законодательства к особенностям расследования данного вида преступлений.

Международное сотрудничество играет ключевую роль в борьбе с транснациональной киберпреступностью, требуя гармонизации законодательств разных стран и развития оперативных механизмов взаимодействия правоохранительных органов.

Особое внимание следует уделить предупреждению вовлечения молодежи в киберпреступную деятельность и усилению защищенности информационных систем.

Перспективным направлением является использование искусственного интеллекта в противодействии киберпреступности, однако, его применение требует тщательного правового регулирования, соблюдения этических норм, развития механизмов общественного контроля, систематического повышения квалификации специалистов и внедрения инновационных технологий с учетом соблюдения прав и свобод граждан.

Конфликт интересов

Не указан.

Рецензия

Все статьи проходят рецензирование в формате double-blind peer review (рецензенту неизвестны имя и должность автора, автору неизвестны имя и должность рецензента). Рецензия может быть предоставлена заинтересованным лицам по запросу.

Conflict of Interest

None declared.

Review

All articles are reviewed in the double-blind peer review format (the reviewer does not know the name and position of the author, the author does not know the name and position of the reviewer). The review can be provided to interested persons upon request.

Литература:

1. Бородкина Т. Н., Павлюк А. В. Киберпреступления: понятие, содержание и меры противодействия // Социально-политические науки. – 2018. – № 1. – С. 135–137.

2. ГОСТ IEC 60050-732–2017. Международный электротехнический словарь. Ч. 732: Терминологии компьютерных сетей. Москва: Стандартинформ, 2020. С. 13.

3. Ивасюк О. Н. Криминологические особенности киберпреступности, направленной против несовершеннолетних // Вестник Санкт-Петербургского университета МВД России. 2021. № 4(92). С. 73-77. https://doi.org/10.35750/2071-8284-2021-4-73-77.

4. Карабеков К. О. Состояние и тенденции киберпреступности в Российской Федерации и Республике Казахстан // Научный вестник Омской академии МВД России. 2024. Т. 30, № 2(93). С. 106-112.

5. Никульченкова Е. В. Проблемы противодействия киберпреступности в России // Психопедагогика в правоохранительных органах. 2023. Т. 28, № 3(94). С. 345-352. https://doi.org/10. 24412/1999-6241-2023-394-345-352.

6. Никульченкова, Е. В. Трансформация киберпреступности: современные угрозы и их предупреждение / Е. В. Никульченкова // Вестник Омского университета. Серия: Право. – 2023. – Т. 20, № 3. – С. 96-105. – DOI 10.24147/1990-5173.2023.20(3).96-105. – EDN JUIJPO.

7. Рычаго, М. Е. Актуальные вопросы определения киберпространства и отражение киберпреступности в зеркале уголовной статистики / М. Е. Рычаго, Д. Н. Никитин // Пенитенциарное право: юридическая теория и правоприменительная практика. – 2023. – № 1(35). – С. 98-103. – EDN ALOEJM.

8. Шикула, И. Р. Киберпреступность в Российской Федерации: основные методы борьбы и проблемы противодействия / И. Р. Шикула, Е. Н. Куркин // Международный журнал экспериментального образования. – 2023. – № 1. – С. 37-41. – DOI 10.17513/mjeo.12119. – EDN CESTGI.

9. Nobles, Calvin & Burton, Sharon & Burrell, Darrell. (2023). Cybercrime as a Sustained Business. 10.4018/978-1-6684-7207-1.ch005. URL: https://www.researchgate.net/publication/369973142_Cybercrime_as_a_Sustained_Business (дата обращения: 13.10.2024).

References:

1. Borodkina T.N., Pavlyuk A.V. Cybercrime: concept, content and counteraction measures. Sotsial'nopoliticheskie nauki. Socio-political sciences. 2018, no. 1, pp. 135-137. (In Russ.).

2. GOST IEC 60050-732-2017. International Electrotechnical Vocabulary. Part 732: Computer Network Terminology. Moscow: Standartinform, 2020. P. 13. (In Russ.).

3. Ivasyuk O.N. Criminological Features of Cybercrime Directed Against Minors. Vestnik Sankt-Peterburgskogo universiteta MVD Rossii. Bulletin of the St. Petersburg University of the Ministry of Internal Affairs of Russia. 2021, no. 4(92), pp. 73-77. (In Russ.). https://doi.org/10.35750/2071-8284-2021-4-73-77

4. Karabekov K. O. State and Tendencies of Cybercrime in the Russian Federation and the Republic of Kazakhstan. Scientific bulletin of the Omsk Academy of the Ministry of the Interior of Russia. 2024. Vol. 30, No 2(93). Pp. 106-112 (In Russ.).

5. Nikulchenkova E.V. Transformation of Cybercrime: Modern Threats and Their Warning. Vestnik Omskogo universiteta. Seriya "Pravo". Herald of Omsk University. Series "Law". 2023, vol. 20, no. 3, pp. 96-105. DOI: 10.24147/1990-5173.2023.20(3).96-105. (In Russ.).

6. Nikulchenkova E. V. Problems of Fighting Cybercrime in Russia. Psychopedagogy in Law Enforcement. 2023. Vol. 28. No. 3(94). Pp. 345-352 (In Russ.). https://doi.org/10.24412/1999-6241-2023-394-345-352

7. Rychago M.E., Nikitin D.N. Topical Issues of Defining Cyberspace and Reflection of Cybercrime in the Mirror of Criminal Statistics. Penitentsiarnoe pravo: yuridicheskaya teoriya i pravoprimenitel'naya

praktika. Penitentiary Law: Legal Theory and Law Enforcement Practice. 2023, no. 1(35), pp. 98-103. (In Russ.).

8. Shikula I.R., Kurkin E.N. Cybercrime in the Russian Federation: Main Methods of Combating and Problems of Counteraction. Mezhdunarodnyi zhurnal eksperimental'nogo obrazovaniya. International Journal of Experimental Education. 2023, no. 1, pp. 37-41. (In Russ.). DOI: 10.17513/mjeo.12119

9. Nobles, Calvin & Burton, Sharon & Burrell, Darrell. (2023). Cybercrime as a Sustained Business. 10.4018/978-1-6684-7207-1.ch005. URL: https://www.researchgate.net/publication/369973142_Cybercrime_as_a_Sustained_Business (accessed: 13.10.2024).

Информация об авторе:

Козаев Нодар Шотаевич, доктор юридических наук, доцент,заместитель начальника филиала по учебной и научной работе, полковник полиции, Ставропольский филиал Краснодарского университета Министерства внутренних дел Российской Федерации

Nodar Sh. Kozaev, Deputy Head of the Branch for Academic and Scientific Work, Doctor of Law, Associate Professor, Police Colonel, Stavropol Branch of Krasnodar University of the Ministry of Internal Affairs of the Russian Federation.