МЕЖДУНАРОДНО-ПРАВОВЫЕ И НАЦИОНАЛЬНЫЕ ПОДХОДЫ К ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПНОСТИ

ТАЗЕТДИНОВ
Руслан Рабинович
Исследовательский институт криминологии
Республики Узбекистан,
доктор философии по психологическим наукам (PhD), доцент,

АГАФОНОВ
Михаил Вячеславович
Всероссийский научно-исследовательский институт
МВД Российской Федерации

Аннотация. *В статье рассматриваются международно-правовые и национальные подходы к противодействию киберпреступности. Анализируются Конвенция ООН против киберпреступности 2024 года, законодательство зарубежных государств и проблемы международного сотрудничества. Выявлены недостатки правового регулирования и предложены меры по совершенствованию уголовного законодательства, развитию цифровой криминалистики и обмену электронными доказательствами.*
Ключевые слова: *киберпреступность, кибермошенничество, международное сотрудничество, Конвенция ООН против киберпреступности, уголовное законодательство, цифровые доказательства, кибербезопасность, трансграничные расследования, цифровая криминалистика, национальная безопасность.*

Annotatsiya. *Ushbu maqola kiberjinoyatchilikka qarshi kurashning xalqaro-huquqiy va milliy yondashuvlarini o'rganadi. Unda 2024-yilgi BMTning Kiberjinoyatchilikka qarshi konventsiyasi, xorijiy davlatlar qonunchiligi va xalqaro hamkorlik bilan bog'liq masalalar tahlil qilinadi. Unda huquqiy tartibga solishdagi kamchiliklar aniqlanadi va jinoyat qonunchiligini takomillashtirish, raqamli sud ekspertizasini rivojlantirish va elektron dalillar almashish bo'yicha choralar taklif etiladi.*
Kalit so'zlar: *kiberjinoyatchilik, kiberfiribgarlik, xalqaro hamkorlik, BMTning Kiberjinoyatchilikka qarshi konventsiyasi, jinoyat huquqi, raqamli dalillar, kiberxavfsizlik, transchegaraviy tergovlar, raqamli sud ekspertizasi, milliy xavfsizlik.*

Abstract. *The article examines international legal and national approaches to combating cybercrime. It analyzes the 2024 UN Convention against Cybercrime, foreign legislation, and problems of international cooperation. Regulatory shortcomings are identified, and measures are proposed to improve criminal legislation, develop digital forensics, and enhance the exchange of electronic evidence.*
Keywords: *cybercrime, cyber fraud, international cooperation, UN Convention against Cybercrime, criminal legislation, digital evidence, cybersecurity, cross-border investigations, digital forensics, national security.*

Анализ современных тенденций новых видов преступлений характерных для зарубежных стран, свидетельствует, об активном росте количества преступлений, совершенных в киберпространстве. Кроме того, «классические» виды преступлений постепенно переплетаются с киберпространством. В этой связи, можно отметить, что кибермошенничество относится к лидирующей форме совершения преступного деяния.

Данный факт подтверждается разработкой по инициативе России и принятием в декабре 2024 года Генеральной Ассамблеей Организации Объединённых Наций Конвенции ООН против киберпреступности (United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of ICT Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes) – первого глобального договора в данной сфере, ставшего результатом многолетних переговоров государств-членов ООН.

Конвенция была открыта для подписания в октябре 2025 года на церемонии высокого уровня в Ханое (Вьетнам). На этой церемонии документ подписали более 65 государств и Европейский Союз, в том числе Узбекистан и Российская Федерация.

Она останется открытой для подписания до конца 2026 года, после чего вступит в силу через 90 дней после того, как его ратифицируют не менее сорока государств.

Также, при проведении анализа стратегий национальной безопасности зарубежных стран, усматривается единая тенденция приоритетности и уделения особого внимания проблемам кибертерроризма, кибератак и преступлений, связанных с киберпространством. Соответственно, данные преступления выделены как несущие прямую угрозу национальной безопасности.

В частности, Стратегия национальной безопасности США определяет, что «к одной значимой задаче обеспечения национальной безопасности относится обеспечение повышения устойчивости к кибератакам, что создает основу для снижения совершения киберпреступлений и стабилизации экономической безопасности США» [6]. Стратегия национальной безопасности ФРГ также определяет «необходимость совершенствования государственной политики в сфере противодействия киберпреступлениям» [7]. Стратегия безопасности Франции предопределяет «необходимость проведения комплекса мероприятий и действий, направленных на защиту от киберугроз» [8]. Концепция глобальной безопасности Китайской Народной Республики, принятая в 2023 г., также указывает на приоритетность «обеспечения защиты от киберпреступлений, как основного вектора развития национальной безопасности» [1].

Таким образом, концепции национальной безопасности зарубежных стран отражают векторы развития государственной политики в сфере противодействия киберпреступлений и кибератак.

Кроме того необходимо отметить, например, Уголовный кодекс ФРГ определяет, что «киберпреступность относится к преступлениям, посягающим на имущественные правоотношения субъектов» [10]. В подтверждение сказанного укажем, что статья 263a УК ФРГ определяет меры уголовной ответственности за совершение компьютерного мошенничества, – лишение свободы сроком до пяти лет либо применение к виновному штрафных санкций. К другому составу киберпреступлений, предусмотренных статьей 303b УК ФРГ, относится компьютерный саботаж. Статья 202a УК ФРГ предусматривает установление уголовной ответственности за противоправное разведывание сведений, совершенное путем сбора и передачи таких сведений с использованием электронных средств.

Таким образом, в Уголовном кодексе ФРГ систематизированы составы киберпреступлений, к числу которых относятся противоправный перехват и завладение информацией; компьютерное мошенничество; компьютерный саботаж. К основной проблеме законодательного регулирования уголовной ответственности следует отнести малозначительность наказания, т.е. применение к виновному лицу лишения

свободы, максимальный срок которого составляет 5 лет, либо штрафных санкций, величина которых определяется судом с учетом тяжести преступления.

Уголовный кодекс Франции также предусматривает привлечение к уголовной ответственности за совершение киберпреступлений. Так, ст. 226–16 Кодекса формирует состав – «противоправное осуществление либо организацию автоматизированной обработки именной информации» [11].

Статья 226-18 УК Франции предусматривает установление самостоятельного состава киберпреступления:

☐ противоправный сбор данных, для которого характерны признаки – обман, самоуправство, применение запрещенного национальным законодательством способа;

☐ противозаконная обработка именной информации физического лица при условии получения несогласия лица на обработку такой информации.

Статья 226–19 УК Франции предусматривает, что к киберпреступлениям относится противоправный ввод либо хранение именной информации без предварительного получения согласия лица.

Основной проблемой правового регулирования ответственности за киберпреступления в УК Франции является отсутствие закрепления самостоятельных составов преступлений, посягающих на частную собственность физических лиц (например, кибермошенничества).

Уголовный кодекс Швейцарии детализирует составы киберпреступлений. Так, ст. 131.1 Кодекса определяет ответственность за «противоправное получение электронных данных, в отношении которых применено требование об усиленной защите; ст. 144 Кодекса – ответственность за совершение действий, направленных на реализацию вредоносных программ в целях противоправного использования, изменения или удаления электронных данных; ст. 147 Кодекса – противоправное вмешательство в электронные данные, совершенное в целях завладения и последующей передачи финансовых активов, либо сокрытия информации о таких действиях» [12].

Основными международным правовым актом, регулирующим вопросы борьбы с киберпреступлениями, является Конвенция ООН против транснациональной организованной преступности. Конвенция определяет требование, согласно которому «государства-участники наделяются полномочиями по заключению как двухсторонних и многосторонних договоров, соглашений в сфере международного сотрудничества по борьбе с преступностью» [2]. Однако, данная Концепция не раскрывает ориентиры международного сотрудничества в сфере противодействия и борьбы с киберпреступностью.

Европейская конвенция о киберпреступлениях [3] детализирует принципы, механизмы и инструменты формирования международного сотрудничества в сфере противодействия и борьбы с исследуемой группой преступлений. Однако, следует указать, что Конвенция не применяется в Российской Федерации, что сдерживает процесс противодействия и борьбы с киберпреступлениями.

Соглашением о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий определяются «векторы формирования и развития международного сотрудничества между странами СНГ и Россией» [5].

Согласно ст. 2 Соглашения, основной целью сотрудничества является создание условий по выявлению, пресечению, раскрытию и предупреждению исследуемой группы преступлений посредством совместного принятия организованно-правовых мер. Основной составляющей, влияющей на оформление международного сотрудничества, как указано в ч. 3 ст. 2 Соглашения, является сближение национального законодательства, регулирующего правоотношения в сфере борьбы с киберпреступлениями.

Таким образом, Соглашением определены основные формы международного сотрудничества, что создает законную основу для повышения эффективности деятельности органов по выявлению, пресечению, раскрытию и предупреждению киберпреступлений.

Особое место в Соглашении уделяется правовому регулированию правоотношений в сфере исполнения запросов об оказании содействия и использованию информации, полученной в рамках такого запроса.

Таллиннское руководство по международному праву, применимому в случае кибервойны определяет «приоритетный принцип международного сотрудничества – формирование нормативной определенности» [9]. Отличительной особенностью Руководства является систематизация киберинцидентов и киберопераций.

Учитывая вышеизложенное, предлагается рассмотреть вопрос о внедрении научных и практических предложений и рекомендации по совершенствованию противодействия киберпреступности:

1. Расширение участия государств в Конвенции ООН против киберпреступности (2024/2025). Учитывая, что Конвенция является первым глобальным и универсальным документом, формирующим единую нормативную основу расследования преступлений, совершаемых с использованием ИКТ, рекомендуется:

- разработать модельные двусторонние и многосторонние соглашения, основанные на механизмах Конвенции, что позволит расширить сотрудничество со странами, не присоединившимися к документу;
- создать специализированную рабочую группу по имплементации Конвенции в национальное законодательство, в том числе по совершенствованию процедур получения электронных доказательств.

2. Гармонизация национального законодательства в соответствии с международными нормами. Опыт стран ЕС, США, Франции, Германии, Швейцарии показывает необходимость:

- сближения правовых определений состава преступлений в сфере ИКТ;
- унификации терминологии (например, «компьютерный саботаж», «несанкционированный доступ», «противоправное получение данных»);
- формализации процедур трансграничного доступа к данным при соблюдении стандартов защиты персональных данных и прав человека.

3. Совершенствование уголовного законодательства:

- формирование системы самостоятельных составов киберпреступлений, ввести отдельные составы преступлений, связанные со всеми этапами кибератаки: получение доступа, модификация данных, создание вредоносного ПО, использование электронных средств для хищений;
- систематизировать преступления по степени общественной опасности (от преступлений против информации до преступлений против собственности и финансовой стабильности);
- пересмотреть санкции: установить дифференцированные сроки лишения свободы, учитывающие масштаб ущерба, трансграничность и степень автоматизации преступной схемы.

4. Развитие цифровой криминалистики. Рекомендуется стандартизировать процедуры фиксации, передачи и хранения цифровых доказательств;

- внедрить сертифицированное программное обеспечение для их анализа;
- разработать методические рекомендации по расследованию преступлений, совершаемых с использованием искусственного интеллекта, deepfake-технологий и автоматизированных систем.

5. Совершенствование системы международного обмена данными:

- создание цифровых шлюзов для обмена электронными доказательствами.

На основе положений Конвенции ООН предлагается: создать единый межгосударственный канал защищённого обмена данными (аналог e-EVIDENCE);

- внедрить электронную систему отслеживания запросов о правовой помощи;
- обеспечить многоуровневую защиту от утечек данных при трансграничной передаче.

Использованные источники

1. Концепция глобальной безопасности Китайской Народной Республики: [Электронный ресурс]. – Режим доступа: https://rg.ru/2023/03/21/davajte-zhit-druzhno.html/.
2. Конвенция против транснациональной организованной преступности (принята в г. Нью-Йорке 15.11.2000 Резолюцией 55/25 на 62-ом пленарном заседании 55-й сессии Генеральной Ассамблеи ООН) (с изм. от 15.11.2000) // Собрание законодательства РФ. 2004. № 40. Ст. 3882.
3. Конвенция о преступности в сфере компьютерной информации (ETS № 185) (Заключена в г. Будапеште 23.11.2001) (с изм. от 28.01.2003): [Электронный ресурс]. – Режим доступа: https://base.garant.ru/4089723/.
4. Сабырбаева, А. Б. Актуальность укрепления международного сотрудничества в борьбе с киберпреступлениями / А. Б. Сабырбаева // Уголовное судопроизводство России и зарубежных государств: проблемы и перспективы развития: материалы международной научно-практической конференции, Санкт-Петербург, 02 декабря 2022 года. – Санкт-Петербург: Санкт-Петербургский университет Министерства внутренних дел Российской Федерации, 2022. – С. 317–323.
5. Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий (Заключено в г. Душанбе 28.09.2018) // Собрание законодательства РФ. 2022. № 33. Ст. 5883.
6. Стратегия национальной безопасности США от 12.10.2022: [Электронный ресурс]. – Режим доступа: https://rdc.grfc.ru/2022/10/usa_national_security_strategy/.
7. Стратегия национальной безопасности Федеральной Республики Германии: [Электронный ресурс]. – Режим доступа: https://translated.turbopages.org/proxy_u/en-ru.ru.cde97a10-6598fb4f-8081bb75-74722d776562/https/www.economist.com/europe/2023/06/15/germanys-new-national-security-strategy-is-strong-on-goals-less-so-on-means/.
8. Стратегия безопасности Франции: [Электронный ресурс]. – Режим доступа: https://tass.ru/mezhdunarodnaya-panorama/16284049/.
9. Таллиннское руководство по международному праву, применимому в случае кибервойны: [Электронный ресурс]. – Режим доступа: https://csef.ru/media/articles/3990/3990.pdf/.
10. Уголовный кодекс Федеративной Республики Германии: [Электронный ресурс]. – Режим доступа: https://constitutions.ru/?p=24969/.
11. Уголовный кодекс Франции: [Электронный ресурс]. – Режим доступа: https://constitutions.ru/?p=25017/.
12. Уголовный кодекс Швейцарии: [Электронный ресурс]. – Режим доступа: https://search.rsl.ru/ru/record/01000960358/.

JINOYATLARNING SABAB VA SHAROITLARINI ANIQLASHDA SUN’IY INTELLEKT TEXNOLOGIYALARIDAN FOYDALANISHNING KRIMINOLOGIK ASOSLARI

TURAYEV
Akmal Panjiyevich
O‘zbekiston Respublikasi Kriminologiya tadqiqot instituti ilmiy xodimi

Annotatsiya. *Ushbu maqolada jinoyatlarning sabab va shart-sharoitlarini aniqlash hamda ularning barvaqt oldini olishda sun’iy intellekt texnologiyalaridan foydalanishning kriminologik asoslari tadqiq etilgan. Tadqiqotda zamonaviy kriminologik nazariyalar nuqtai nazaridan jinoyatchilikka ta’sir etuvchi omillarni tahlil qilish imkoniyatlari yoritilgan. Shuningdek, AQSH, Buyuk Britaniya, Xitoy, Germaniya va Singapurda qo‘llanilayotgan sun’iy intellekt tizimlarining samaradorligi, huquqiy va axloqiy jihatlari tahlil qilingan. O‘zbekistonda jinoyatchilikni prognoz qilish va profilaktika qilish sohasiga sun’iy intellekt texnologiyalarini joriy etishning institutsional, huquqiy va texnologik asoslari asoslantirilib, milliy “Criminology AI” platformasini ishlab chiqish bo‘yicha takliflar ilgari surilgan.*
Kalit so‘zlar: *sun’iy intellekt, kriminologiya, prediktiv politsiya, jinoyat sabablari, avtomatik o‘qitish, neyron tarmoq, jinoyat xaritasi, algoritmik xolislik, profilaktika, COMPAS, Pred Pol, Hunch Lab, Shot Spotter, xorijiy tajriba, huquqiy tartibga solish.*

Аннотация. *Данная статья рассматривает криминологические основы использования технологий искусственного интеллекта для выявления причин и условий преступлений и обеспечения их ранней профилактики. В исследовании подчеркивается потенциал анализа факторов, влияющих на преступность, с точки зрения современных криминологических теорий. Анализируется эффективность, правовые последствия и этические аспекты систем искусственного интеллекта, применяемых в США, Великобритании, Китае, Германии и Сингапуре. Обосновываются институциональные, правовые и технологические основы внедрения технологий искусственного интеллекта в прогнозирование и предотвращение преступлений в Узбекистане и предлагаются рекомендации по развитию национальной платформы «Criminology AI».*
Ключевые слова: *искусственный интеллект, криминология, предиктивная полиция, причины преступности, машинное обучение, нейронная сеть, карта преступности, алгоритмическая беспристрастность, профилактика, COMPAS, PredPol, HunchLab, ShotSpotter, зарубежный опыт, правовое регулирование.*

Abstract. *This article examines the criminological foundations of the use of artificial intelligence technologies in identifying the causes and conditions of crimes and ensuring their early prevention. The study highlights the potential for analyzing factors influencing criminality from the perspective of contemporary criminological theories. Furthermore, it analyzes the effectiveness, legal implications, and ethical aspects of artificial intelligence systems employed in the United States, the United Kingdom, China, Germany, and Singapore. The article substantiates the institutional, legal, and technological foundations for the implementation of artificial intelligence technologies in crime prediction and prevention in Uzbekistan and proposes recommendations for the development of the national “Criminology AI” platform.*
Keywords: *artificial intelligence, criminology, predictive policing, causes of crime, machine learning, neural network, crime mapping, algorithmic fairness, crime prevention, COMPAS, PredPol, HunchLab, ShotSpotter, foreign experience, legal regulation.*