DOI: 10.47026/2499-9636-2026-1-90-96

УДК 343.9:004.056
ББК Х410.21 + Х403.3

А.В. КУРАКОВ

ПРЕСТУПЛЕНИЯ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ В УГОЛОВНОМ ЗАКОНОДАТЕЛЬСТВЕ ЗАРУБЕЖНЫХ СТРАН

Ключевые слова: *киберпреступность, информационно-телекоммуникационные сети, уголовное законодательство, сравнительное правоведение, компьютерные преступления, правовая модель, транснациональное сотрудничество, Будапештская конвенция.*

Тотальная цифровизация и повсеместная интеграция информационно-телекоммуникационных сетей в социально-экономические процессы создают принципиально новую среду для противоправной деятельности. Киберпреступления представляют собой транснациональную угрозу безопасности, экономике и правам человека. Скорость технологических изменений существенно опережает законотворческий процесс, из-за чего правовое регулирование остается фрагментарным, а его применение – затрудненным, особенно ввиду трансграничной природы современных киберугроз. В связи с этим сравнительно-правовой анализ зарубежных моделей криминализации в данной сфере представляется актуальным.

Цель исследования *– выявить основные модели криминализации киберпреступлений в уголовном законодательстве зарубежных государств, определить системные закономерности их развития (включая тенденцию к конвергенции) и установить характерные национальные особенности формирующейся глобальной модели регулирования.*

Материалы и методы. *В основе работы лежит сравнительно-правовой, формально-юридический и историко-правовой анализ. Исследование опирается на тексты законов США, Великобритании, Китая, ЕС, международных конвенций и научную литературу.*

Результаты. *В мировой практике сформировались две основные модели криминализации киберпреступлений: интегративная (путем дополнения традиционных уголовных кодексов) и комплексная (на основе специализированных законов). В настоящее время наблюдается тенденция к их конвергенции и формированию гибридной модели. В результате сопоставления национальных правовых систем были выявлены ключевые особенности уголовно-правового регулирования киберпреступлений. В США акцент сделан на защите экономических интересов и критической инфраструктуры при широком толковании понятия «несанкционированный доступ». В праве Европейского союза доминирует гармонизация законодательства на основе Будапештской конвенции с приоритетом защиты приватности (GDPR). Китайская модель характеризуется жестким государственным контролем киберпространства и криминализацией распространения «вредной информации» в целях защиты суверенитета. Происходит экспансия объекта уголовно-правовой охраны на новые цифровые ценности (криптоактивы, целостность алгоритмических систем). Отмечена тенденция к криминализации подготовительных деяний, усилению защиты критической информационной инфраструктуры путем введения квалифицированных составов, а также интеграции норм о киберпреступлениях в контекст борьбы с организованной преступностью. Установлено, что эффективность противодействия зависит не только от законодательных норм, но и от технологических возможностей правоприменения и уровня развития трансграничного сотрудничества.*

Выводы. *Уголовное законодательство в сфере информационно-телекоммуникационных сетей демонстрирует глобальную конвергенцию подходов: формируется гибридная модель, ядром которой служат международные стандарты (Будапештская конвенция), а национальные особенности определяют специфические приоритеты (экономика в США, приватность в ЕС, суверенитет в Китае). Ключевой тренд – переход от реакции на инциденты к превентивному регулированию, включая криминализацию подготовительных действий. Однако окончательная эффективность борьбы зависит не столько от жесткости законов, сколько от способности правоприменителей работать с цифровыми доказательствами, налаживать трансграничное сотрудничество и соблюдать баланс между безопасностью и фундаментальными правами человека в цифровой среде.*

Введение. Цифровая трансформация общества, характеризующаяся тотальной интернетизацией и интеграцией информационно-телекоммуникационных сетей (ИТС) во все сферы жизнедеятельности, сформировала новый, виртуальный ландшафт криминальной активности. Преступления с использованием ИТС, или киберпреступления, перестали быть узкоспециальной проблемой и стали одной из ключевых угроз национальной и международной безопасности, экономической стабильности и правам личности [5. С. 34].

Ответом правовых систем на этот вызов стала активная модернизация уголовного законодательства. Однако скорость технологических изменений часто опережает законодательный процесс, что приводит к фрагментарности правового регулирования и проблемам правоприменения. В этой связи изучение зарубежного опыта становится не только академически значимым, но и практически востребованным для совершенствования отечественного правового механизма противодействия киберпреступности [2].

Цель исследования – выявить основные модели криминализации киберпреступлений в уголовном законодательстве зарубежных государств, определить системные закономерности их развития (включая тенденцию к конвергенции) и установить характерные национальные особенности формирующейся глобальной модели регулирования.

Материалы и методы. Методологическую основу исследования составляют общенаучные (анализ, синтез, индукция, дедукция, сравнение) и специальные юридические методы познания. Ведущим выступил сравнительно-правовой метод, примененный для сопоставления уголовно-правовых норм, направленных против киберпреступности, в различных национальных системах (США, Великобритания, Китай, Россия, страны ЕС) и на международном уровне. Формально-юридический метод использовался для анализа структуры и содержания конкретных нормативных актов, таких как U.S. Computer Fraud and Abuse Act, британский Computer Misuse Act 1990, Уголовный кодекс КНР, Будапештская конвенция Совета Европы о киберпреступности (2001 г.) и директивы Европейского союза. Историко-правовой метод позволил проследить эволюцию законодательного регулирования от первых законов 1970-х гг. до современных комплексных актов. Материалами исследования послужили тексты международных конвенций, национальных законов и подзаконных актов, а также научные источники (монографии, статьи) по проблемам киберпреступности и сравнительного уголовного права.

Результаты исследования. Формирование правового регулирования киберпреступлений относится к 1970–1980-м гг., когда благодаря технологическому прогрессу появились предпосылки для хищения данных и вмешательства в работу ЭВМ. США выступили пионером в этой области, приняв первый специализированный закон «Florida Computer Crimes Act»[1] в 1978 г., а на федеральном уровне в 1984 г. – «Computer Fraud and Abuse Act»[2], который заложил основы американской системы противодействия компьютерным преступлениям.

[1] Florida Computer Crimes Act: § 815.04, Florida Statutes (2025). Available at: https://www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&URL=0800-0899/0815/0815.html (Access Date: 2026, Jan. 24).

[2] Computer Fraud and Abuse Act. 18 U.S.C. § 1030. Available at: https://www.justice.gov/jm/jm-9-48000-computer-fraud (Access Date: 2026, Jan. 24).

Сформировались две основные модели криминализации. Интегративная (эволюционная) модель заключается во внедрении новых составов преступлений, связанных с ИТС, в текст действующего традиционного уголовного кодекса путем его дополнения или модификации. Эта модель характерна для стран континентальной правовой семьи, таких как Германия, Франция, Испания и Россия. Ее преимущество состоит в сохранении системности и доктринальных основ уголовного права, а недостаток – в возможном несоответствии устоявшихся юридических конструкций (например, понятия «имущество») новым цифровым реалиям, таким как данные и криптоактивы. Вторая модель – комплексная (революционная) – предполагает принятие отдельного специализированного законодательного акта, посвященного исключительно компьютерным или информационным преступлениям. Эта модель широко распространена в странах общего права (например, в Великобритании действует Computer Misuse Act 1990[1]), а также в ряде азиатских государств, в частности в Сингапуре, где принят Computer Misuse and Cybersecurity Act[2], включающий положения о кибербезопасности. Подход, заложенный в подобных специализированных актах, позволяет привлекать к уголовной ответственности не только за совершение оконченного киберпреступления, но и за сам факт организации или участия в преступном сговоре. Как отмечается И.Н. Мосечкиным, «лица, объединившиеся для совершения противоправных деяний, привлекаются к ответственности независимо от того, удалось ли им достигнуть желаемых результатов» [6]. Комплексная модель позволяет более гибко и детально регулировать специфические отношения, однако может создавать коллизии с общими нормами уголовного кодекса. На практике наблюдается конвергенция этих моделей: страны с интегративной моделью принимают специализированные законы о данных или кибербезопасности, а страны с комплексной моделью ссылаются на общие нормы уголовного кодекса при квалификации сопутствующих преступлений, таких как вымогательство или мошенничество.

Сравнительный анализ уголовно-правовых систем различных стран выявляет их ключевые особенности. Американское законодательство о компьютерных преступлениях базируется на Computer Fraud and Abuse Act[3] и характеризуется широким понятием «несанкционированный доступ» к защищенному компьютеру, которое подвергается критике за чрезмерную карательность и правовую неопределенность, так как позволяет привлекать к ответственности даже за действия с общедоступными данными, если доступ к ним был получен «без разрешения» [3]. Акцент в США сделан на защите экономических интересов и критической инфраструктуры. При этом, как отмечается в исследовании, в американском законодательстве отсутствует единое определение преступлений против электронной информации, а уровень кодификации в этой области признается достаточно низким.

[1] Computer Misuse Act 1990. P. 18. Available at: https://www.legislation.gov.uk/ukpga/1990/18/contents (Access Date: 2026, Jan. 24).
[2] Computer Misuse Act 1993. Chapter 50A. Available at: https://sso.agc.gov.sg/Act/CMA1993 (Access Date: 2026, Jan. 24).
[3] Computer Fraud and Abuse Act. 18 U.S.C. § 1030 Available at: https://www.justice.gov/jm/jm-9-48000-computer-fraud (Access Date: 2026, Jan. 24).

Правовое пространство Европейского Союза стремится к максимальной гармонизации национальных законодательств, отправной точкой стала Будапештская конвенция 2001 г.[1] Европейская модель сочетает классические составы киберпреступлений с мощным акцентом на превентивную защиту систем и приватности, что отражено в таких документах, как Директива NIS2 и Общий регламент по защите данных. Однако, как показывает анализ, «по мере развития информационных технологий совершенствуются имеющиеся и разрабатываются новые меры по противодействию преступлениям экономической направленности» [4]. Это находит отражение в постоянной эволюции европейских директив, таких как заменившая устаревшее Рамочное решение Директива (ЕС) 2019/713, которая установила более жесткие требования в отношении оперативного реагирования, уведомления правоохранительных органов и стимулирования сообщений о киберпреступлениях. Европейская модель сочетает классические составы киберпреступлений с мощным акцентом на превентивную защиту систем и приватности, что отражено в таких документах, как Директива NIS2[2] и Общий регламент по защите данных (GDPR)[3].

Китайский подход характеризуется жестким государственным контролем над киберпространством и приоритетом защиты национальной безопасности и общественного порядка, включая криминализацию распространения «вредной информации» в сети. Это является частью комплексной стратегии, в рамках которой Интернет рассматривается как ключевой сектор государственной инфраструктуры и суверенное пространство, требующее защиты от внешнего воздействия. Как отмечает ряд исследователей [1], кибербезопасность КНР обеспечивается не только законодательными запретами, но и активным развитием национальных информационных технологий, созданием специализированных кибернетических воинских подразделений (таких как «Голубая кибермия»), а также сотрудничеством государства с бизнес-структурами и техническими вузами для разработки собственных критических технологий. Стратегия направлена на достижение технологического доминирования и цифрового суверенитета, что включает контроль над внутренним интернет-пространством (в том числе над системой доменных имен) и пропагандистскую работу для формирования положительного образа страны за рубежом. Большинство государств-участников СНГ пошли по пути интегративной модели, дополнив свои уголовные кодексы статьями, аналогичными нормам Будапештской конвенции, с недавним смещением акцента на криминализацию кардинга и преступлений, связанных с криптовалютами.

---

[1] Конвенция о киберпреступности: [заключена в г. Будапешт 23.11.2001] [Электронный ресурс]. URL: https://base.garant.ru/4089723/ (дата обращения: 24.01.2026).

[2] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555 (Access Date: 2026, Jan. 24).

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj (Access Date: 2026, Jan. 24).

Анализ современного зарубежного законодательства позволяет выделить ряд общих тенденций. Происходит экспансия объекта уголовно-правовой охраны, включающая теперь не только данные и системы, но и целостность цифровых услуг, доверие к алгоритмическим системам, «цифровой покой» личности и криптоактивы. Наблюдается криминализация «подготовительных» деяний, когда устанавливается ответственность за создание или распространение инструментов для киберпреступлений даже при отсутствии последующих атак. Усиливается защита критической информационной инфраструктуры с введением квалифицированных составов и более суровых санкций. Нормы о киберпреступлениях интегрируются в контекст борьбы с организованной и террористической деятельностью. Активно развиваются механизмы экстерриториальной юрисдикции и международного сотрудничества, включая создание совместных киберподразделений и упрощенных каналов обмена электронными доказательствами. Вместе с тем сохраняются ключевые вызовы, такие как проблема атрибуции атак, правовое регулирование действий «хакеров в законе», обеспечение баланса между безопасностью и шифрованием, а также необходимость защиты фундаментальных прав и свобод.

Выводы. Уголовное законодательство зарубежных стран находится в состоянии динамичной адаптации к вызовам цифровой эпохи и демонстрирует конвергенцию подходов. Формируется конвергентная глобальная модель, ядро которой составляют нормы, направленные на защиту конфиденциальности, целостности и доступности данных и систем, а также на борьбу с компьютерным мошенничеством. В данное ядро интегрируются специфические национальные особенности: акцент на экономическую безопасность в США, на приватность и гармонизацию в ЕС, на государственный суверенитет в Китае. Ключевой тенденцией является переход от реагирования на инциденты к созданию комплексной упреждающей системы охраны. Однако ее эффективность зависит не только от строгости законов, но и от способности правоприменительных органов работать с цифровыми доказательствами и развивать трансграничное сотрудничество.

Для совершенствования отечественного законодательства целесообразно углубленное изучение европейского опыта гармонизации, механизмов быстрого реагирования и моделей публично-частного партнерства.

Литература

1. *Каспарян К.В., Рутковская М.В.* Специфические черты и перспективы развития электронного правительства в КНР в начале XXI столетия // Философские проблемы информационных технологий и киберпространства. 2021. № 2(20). С. 61–83.

2. Киберпреступность и уголовная политика: монография / под ред. А.И. Рарога. М.: Проспект, 2021. 304 с.

3. *Кушхов А.А.* Зарубежный опыт обеспечения безопасности электронной информации уголовно-правовыми средствами (на примере США) // Вестник Саратовской государственной юридической академии. 2024. № 4(159). С. 135–141.

4. *Лунеев В.В.* Преступность XX века: мировые, региональные и российские тенденции. 2-е изд., перераб. и доп. М.: Норма, 2019. 912 с.

5. *Мосечкин И.Н.* Уголовная ответственность за организацию устойчивой группы лиц, созданной для совершения преступлений в сфере компьютерной информации // Вестник Санкт-Петербургского университета. Сер. 14. Право. 2022. № 1. С. 28–45.

6. *Щербакова А.В.* Международно-правовое регулирование противодействия преступлениям экономической направленности, совершаемые посредством использования IT-технологий // Государственная служба и кадры. 2025. № 3. С. 220–223.

КУРАКОВ АНТОН ВЯЧЕСЛАВОВИЧ – аспирант кафедры уголовно-правовых дисциплин, Чувашский государственный университет, Россия, Чебоксары (kurakovbanton@gmail.com).

Anton V. KURAKOV

CRIMES INVOLVING THE USE OF INFORMATION AND TELECOMMUNICATION NETWORKS IN THE CRIMINAL LEGISLATION OF FOREIGN COUNTRIES

Key words: *cybercrime, information and telecommunication networks, criminal law, comparative law, computer crimes, legal model, transnational cooperation, Budapest Convention.*

Total digitalization and a widespread integration of information and telecommunication networks into socio-economic processes create a fundamentally new environment for illegal activities. Cybercrimes pose a transnational threat to security, the economy and human rights. The pace of technological change is far outstripping the legislative process, with the result that legal regulation remains piecemeal and its application is hampered, particularly given the cross-border nature of modern cyber threats. In this context, a comparative legal analysis of foreign models of criminalisation in this area appears to be relevant.

The purpose of the study *is to identify the main models cybercrimes criminalization in the criminal legislation of foreign countries, to identify the systemic patterns of their development (including the tendency towards convergence) and to identify the characteristic national features of the emerging global regulatory model.*

Materials and methods. *The work is based on comparative-legal, formal-legal and historical-legal analysis. The research is based on the texts of the laws of the USA, Great Britain, China, the EU, international conventions and scientific literature.*

Results. *Two main models for cybercrimes criminalisation have emerged in the international practice: the integrative model (by amending traditional criminal codes) and the comprehensive model (based on specialised laws). Currently, there is a tendency for their convergence and forming a hybrid model. As a result of the comparison of national legal systems, the key features of the criminal law regulation of cybercrime were identified. In the US, the focus is on protecting economic interests and critical infrastructure, with a broad interpretation of the term "unauthorized access". European Union law is dominated by the harmonization of legislation based on the Budapest Convention with the priority of protecting privacy (GDPR). The Chinese model is characterized by strict state control of cyberspace and criminalization of disseminating "harmful information" in order to protect sovereignty. The object of criminal law protection is expanding to new digital values (cryptoassets, integrity of algorithmic systems). There has been a trend towards criminalising preparatory acts, strengthening the protection of critical information infrastructure through introduction of aggravated offences, and integrating provisions on cybercrime into the broader context of the fight against organised crime. It was established that the effectiveness of counteraction depends not only on legislative norms, but also on the technological capabilities of law enforcement and the level of cross-border cooperation development.*

Conclusions. *Criminal legislation in the field of information and telecommunications networks demonstrates a global convergence of approaches: a hybrid model is emerging, centred on international standards (the Budapest Convention), whilst national characteristics determine specific priorities (the economy in the US, privacy in the EU, sovereignty in China). The key trend is the transition from incident response to preventive regulation, including criminalization of preparatory actions. However, the ultimate effectiveness of the fight against crime depends not so much on the strictness of the laws as on the ability of law enforcement agencies to handle digital evidence, establish cross-border cooperation and strike a balance between security and fundamental human rights in the digital environment.*

References

1. Kasparian K.V., Rutkovskaia M.V. *Spetsificheskie cherty i perspektivy razvitiia pravitel'stva v KNR v nachale XXI veka* [Specific features and development prospects of the government in the PRC at the beginning of the 21st century]. *Filosofskie problemy informatsionnykh tekhnologii i kiberprostranstva*, 2021, no. 2(20), pp. 61–83.

2. Rarog A.I., ed. *Kiberprestupnost' i ugolovnaia politika* [Cybercrime and criminal policy]. Moscow, Prospekt Publ., 2021. 304 p.

3. Kushkhov A.A. *Zarubezhnyi opyt obespecheniia elektronnoi informatsionno-pravovoi pomoshchi (na primere SShA)* [Foreign experience in providing electronic information and legal assistance (the example of the USA)]. *Vestnik Saratovskoi gosudarstvennoi iuridicheskoi akademii*, 2024, no. 4(159), pp. 135–141.

4. Luneev V.V. *Kurs mirovoi i rossiiskoi kriminologii* [Course of world and Russian criminology]. Moscow, Norma Publ., 2019. 912 p.

5. Mosechkin I.N. *Ugolovnaia otvetstvennost' za organizatsiiu ustoichivoi gruppy lits, sozdannoi dlia soversheniia prestuplenii v sfere komp'iuternoi informatsii* [Criminal liability for the organization of a stable group of persons created to commit crimes in the sphere of computer information]. *Vestnik Sankt-Peterburgskogo universiteta. Seriia 14. Pravo*, 2022, no. 1, pp. 28–45.

6. Shcherbakova A.V. *Mezhdunarodno-pravovoe regulirovanie protivodeistviia virusam ekonomicheskoi napravlennosti, osushchestvliaemoe za schet ispol'zovaniia IT-tekhnologii* [International legal regulation of combating economic viruses through the use of IT technologies]. *Gosudarstvennaia sluzhba i kadry*, 2025, no. 3, pp. 220–223.

ANTON V. KURAKOV – Post-Graduate Student, Department of Criminal Law Disciplines, Chuvash State University, Russia, Cheboksary (kurakovbanton@gmail.com).

Формат цитирования: *Кураков А.В.* Преступления с использованием информационно-телекоммуникационных сетей в уголовном законодательстве зарубежных стран [Электронный ресурс] // Oeconomia et Jus. 2026. № 1. С. 90–96. URL: http://oecomia-et-jus.ru/single/2026/1/8. DOI: 10.47026/2499-9636-2026-1-90-96.