Уголовная ответственность за киберпреступления в законодательстве зарубежных стран

Criminal liability for cybercrimes in the legislation of foreign countries

DOI: 10.12737/2500-333X-2026-11-2-150-156

Кравчук Е.А.
Обучающаяся 2 курса по направлению подготовки 40.05.04 «Судебная и прокурорская деятельность», Дальневосточный филиал ФГБОУВО «Российская государственная университет правосудия имени В.М. Лебедева», г. Хабаровск
e-mail: kravchukoa7@gmail.com

Kravchuk E.A.
2nd-year student in the program 40.05.04 "Judicial and Prosecutor's Activity", Far Eastern Branch of the V.M. Lebedev Russian State University of Justice, Khabarovsk
e-mail: kravchukoa7@gmail.com

Коротченков Д.А.
Канд. юрид. наук, доцент кафедры уголовно-правовых дисциплин, Дальневосточный филиал ФГБОУВО «Российский государственный университет правосудия имени В.М. Лебедева», г. Хабаровск
e-mail: korotchenkov.d@mail.ru

Korotchenkov D.A.
Candidate of Law, Associate Professor, Department of Criminal Law, Far Eastern Branch of the V.M. Lebedev Russian State University of Justice, Khabarovsk
e-mail: korotchenkov.d@mail.ru

Аннотация
В данной статье рассматриваются особенности уголовной ответственности за киберпреступления в условиях цифровизации и глобализации информационного пространства. Анализируется актуальность уголовной ответственности за преступления в цифровой среде как на национальном, так и на международном уровне. Особое внимание уделяется анализу научных подходов различных авторов в современной юридической науке к определению понятия «киберпреступление», характеристику его основных признаков, на основе данных подходов формулируется авторское понятие. На основе сравнительно-правого анализа законодательства США, Германии, Японии, Китая и Ирана выявляются основные модели уголовно-правового регулирования киберпреступлений. В рамках проведенного исследования выявляются основные тенденции развития уголовного законодательства в сфере киберпреступности в зарубежных странах и формируются предложения по совершенствованию уголовного законодательства Российской Федерации.
Ключевые слова: уголовное право, киберпреступления, уголовная ответственность, цифровая среда, информационно-телекоммуникационные технологии, кибербезопасность, зарубежное законодательство.

Abstract
This article discusses the specifics of criminal liability. for cybercrimes in the context of digitalization and globalization of the information space. The relevance of criminal liability for crimes in the digital environment is analyzed both at the national and international levels. Special attention is paid to the analysis of scientific approaches of various authors in modern legal science to the definition of the concept of "cybercrime", the characteristics of its main features, on the basis of these approaches the author's concept is formulated. Based on a comparative legal analysis of the legislation of the USA, Germany, Japan, China and Iran, the main models of criminal law regulation of cybercrime are identified. The study identifies the main trends in the development of criminal legislation in the field of cybercrime in foreign countries and forms proposals for improving the criminal legislation of the Russian Federation.
Keywords: cybercrimes, criminal liability, digital environment, information and telecommunication technologies, cybersecurity, foreign legislation.

В условиях стремительного развития цифровых технологий и глобализации информационного пространства киберпреступность становится одной из наиболее серьезных угроз национальной безопасности Российской Федерации. Современные информационно-телекоммуникационные сети активно используются не только в легальной деятельности, но и в преступных целях, что обуславливает рост числа преступлений, совершаемых с использованием компьютерных технологий. В связи с этим проблема уголовной ответственности за киберпреступления приобретает особую актуальность как на национальном, так и на международном уровне.

Изучение уголовной ответственности за киберпреступления в законодательстве зарубежных стран имеет важное теоретическое и практическое значение. Оно способствует выработке эффективных механизмов противодействия преступлениям в цифровой среде и может быть использовано при совершенствовании национального уголовного законодательства с учетом положительного зарубежного опыта.

Для комплексного и системного изучения уголовной ответственности за киберпреступления на первоначальном этапе исследования представляется необходимым обратиться к анализу понятия и основных признаков киберпреступлений, что позволит выявить их правовую природу и особенности как объекта уголовно-правового регулирования.

Доктринальное использование термина «киберпреступления» оправданно, поскольку обозначает принадлежность этого понятия к отрасли уголовного права. Юридической наукой еще не выработано какого-либо комплексного взгляда на правовую природу и особенности данного понятия.

В современном уголовном праве отсутствует универсальное и общепризнанное определение киберпреступления, что обусловлено быстрым развитием цифровых технологий и разнообразием форм преступного поведения в информационном пространстве. Различные ученые определяют данное понятие по-разному, приведем некоторые примеры.

Карпова Д.Н. в своем исследовании указывает, что «киберпреступление – это акт социальной девиации с целью нанесения экономического, политического, морального, идеологического, культурного и других видов ущерба, индивиду, организации или государству посредствам любого технического средства с доступом в Интернет» [7, с. 163].

М.А. Простосердов использует термин «киберпространство» для раскрытия содержания понятия «киберпреступление». По мнению данного автора «под киберпреступлением понимается преступление, причиняющее вред разнородным общественным отношениям, совершаемое дистанционно, путём использования средств компьютерной техники и информационно-телекоммуникационных сетей и образованного ими киберпространства» [9, с. 43].

Так, Е.П. Ищенко считает, что под «киберпреступностью понимаются преступления в сфере высоких информационных технологий, совершаемые злоумышленниками, использующими эти технологии в противоправных целях» [4, с. 336].

Таким образом, основываясь на изложенном, с учетом различных научных подходов к определению понятия «киберпреступление», авторами было сформулировано авторское понятие. Киберпреступление – это общественно опасное, виновное, противоправное деяние, совершаемое с использованием компьютерных технологий, информационных систем связей и киберпространства, направленное на причинение вреда личности, обществу и государству в экономической, политической, информационной и иных сферах.

Говоря о признаках киберпреступлений, Клишков В.Б., Стебенева Е.В., Яковлева М.А. отмечают, что: «Характерными признаками киберпреступлений являются не только общественная опасность, но и оперативность совершения деяния, удаленность, а также масштабность и высокая анонимность, отражающаяся не только в сложности обнаружения виновного, но и в вероятности предоставить информацию потребителю, не соответствующую действительности. Такой признак киберпреступности, как самодостаточность, облегчает совершение и сокрытие посягательства, а признак виртуальности характеризует место деяния в качестве идеальной не опознанной с точностью среды для «трансформации» личности преступника, перевоплощения и корректирования характеристик (внешнего вида и пр.)» [5, с. 107].

И.Г. Чекунов на основе анализа отечественных и международных нормативных правовых актов, говоря о признаках киберпреступлений, указывает, что: «Цели преступников достигаются с помощью средств информационных коммуникационных технологий, последствия от подобных преступлений имеют реальный характер, киберпреступления обладают трансграничным характером и совершаются виртуальными способами, киберпреступления не являются очевидными, совершаются скрытно, сбор доказательств, касающихся таких преступлений, затруднительный» [8, с. 251].

Иванова Л.В. выделяет следующие признаки киберпреступлений: «Объективная сторона характеризуется использованием компьютерной техники и информационно-телекоммуникационных сетей для совершения преступления; объектами посягательств выступают общественные отношения в сфере обеспечения безопасности обращения компьютерной информации, а также общественные отношения, связанные с такой информацией и одновременно с реальным миром; субъект киберпреступления обладает специальными познаниями в сфере компьютерной техники и информационных технологий либо использует специальные программные комплексы для совершения неправомерных деяний; субъективная сторона характеризуется наличием у лица преступного умысла» [1].

Также, по мнению ряда авторов, говоря о признаках киберпреступлений, следует добавить такие признаки, как использование цифровой среды в качестве средства или объекта посягательства; значительный ущерб, причиняемый как отдельным лицам, так и государству в целом. Данные признаки обуславливают специфику уголовно-правового регулирования и необходимость особых подходов к формированию составов преступления.

Далее рассмотрим особенности уголовной ответственности за киберпреступления в зарубежных странах.

В 1977 г. в США был разработан законопроект о защите федеральных компьютерных систем, устанавливающий уголовную ответственность за:

- введение недостоверной информации в компьютерную систему;
- противозаконное применение компьютерных устройств;
- изменение процессов обработки информационных данных либо нарушение указанных процессов;
- хищение денег, ценных бумаг, имущества, ценной и другой информации с применением потенциала компьютерных технологий [6].

На основе данного законопроекта в октябре 1984 г. был принят закон о мошенничестве и злоупотреблении с использованием компьютеров (Computer Fraud and Abuse Act (далее – CFAA) – основной нормативно-правовой акт, устанавливающий уголовную ответственность за преступления в сфере компьютерной информации) [2].

В приведенной ниже табл. кратко изложены различные подразделы раздела 1030 (CFAA) и соответствующие им сроки наказания:

Преступление	Раздел	Наказание
Получение информации, касающейся национальной безопасности	1030(a)(1)	За первое преступление предусмотрено наказание в виде лишения свободы на срок 10 лет, для повторных нарушений – до 20 лет
Доступ к компьютеру и получение информации	1030(a)(2)	За первое преступление предусмотрено наказание в виде лишения свободы на срок от 1 года до 5 лет, для повторных нарушений – 10 лет
Несанкционированный доступ к правительственному компьютеру	1030(a)(3)	За первое преступление предусмотрено наказание в виде лишения свободы на срок 1 год, для повторных нарушений – до 10 лет
Использование компьютера для мошенничества и получения выгоды	1030(a)(4)	За первое преступление предусмотрено наказание в виде лишения свободы на срок 5 лет, для повторных нарушений – до 10 лет
Умышленное причинение вреда путем осознанной передачи	1030(a)(5)(A)	За первое преступление предусмотрено наказание в виде лишения свободы на срок от 1 года до 10 лет, для повторных нарушений – до 20 лет
Безрассудное причинение вреда путем преднамеренного доступа	1030(a)(5)(Б)	За первое преступление предусмотрено наказание в виде лишения свободы на срок от 1 года до 5 лет, для повторных нарушений – до 20 лет
Неосторожное причинение ущерба и убытков в результате умышленного доступа	1030(a)(5)(C)	За первое преступление предусмотрено наказание в виде лишения свободы на срок 1 год, для повторных нарушений – до 10 лет
Торговля паролями	1030(a)(6)	За первое преступление предусмотрено наказание в виде лишения свободы на срок 1 год, для повторных нарушений – до 10 лет
Вымогательство с использованием компьютера	1030(a)(7)	За первое преступление предусмотрено наказание в виде лишения свободы на срок 5 лет, для повторных нарушений – до 10 лет

Таблица подразделов раздела 1030 (CFAA) [13]
The subsection table of section 1030 (CFAA) [13]

Также стоит отметить, что в 2015 г. Конгресс США принял закон о кибербезопасности, приравнявший компьютерные и реальные преступления. За шпионаж и хищение интеллектуальной собственности грозит до 20 лет тюрьмы, за проникновение в критическую инфраструктуру – до 30 лет без досрочного освобождения [6].

В Уголовном кодексе Германии (Strafgesetzbuch, (далее – StGB) нет отдельного раздела о преступлениях в сфере компьютерной информации, но есть нормы, которые предусматривают ответственность за деяния, которые связаны с использованием компьютерных средств.

Так, § 202a StGB устанавливает ответственность за незаконное получение данных и предусматривает наказание в виде лишения свободы до трех лет или штрафом; § 202b StGB устанавливает ответственность за перехват данных и наказывается лишением свободы на срок до двух лет или штрафом, если только данное деяние не предусматривает более сурового наказания в соответствии с другими положениями; § 202c StGB устанавливает ответственность за подготовку к слежке и перехвату данных и наказывается лишением свободы на срок до двух лет или штрафом [15].

За незаконное изменение или уничтожение данных ответственность предусмотрена §303a StGB и наказывается лишением свободы до двух лет и штрафом, а за нарушение функционирования компьютерных систем – §303b StGB, предусматривающий лишение свободы до трех лет, а при причинении значительного ущерба или посягательстве на критически важные системы – до десяти лет [15]. Компьютерное мошенничество регулируется §263a StGB и наказывается лишением свободы от трех до пяти лет или штрафом [15].

В Японии уголовная ответственность за киберпреступления носит комбинированный характер и регулируется как нормами Уголовного кодекса Японии (Кэйхо), так и специальным законодательством. Ключевым актом является Закон о запрете несанкционированного компьютерного доступа 2000 г. (Unauthorized Computer Access Act). Например: ст. 3 – запрещает незаконный доступ к компьютеру и предусматривает наказание лишением свободы с принудительными работами на срок не более трех лет или штрафом в размере не более 1 миллиона иен, ст. 4-7 – запрещают незаконное получение, хранение и использование чужих идентификационных кодов и предусматривает наказание лишением свободы с принудительными работами на срок не более одного года или штрафом в размере не более 500 000 иен (ст.12) [11].

Уголовный кодекс Японии также содержит специальные нормы, направленные на борьбу с киберпреступлениями (например, ст. 161-2 – несанкционированное создание электронных или магнитных записей, наказание лишением свободы на срок не более 5 лет или штрафом в размере не более 1 000 000 иен; ст. 234-2 – воспрепятствование деятельности предприятия путем повреждения компьютера, наказание лишение свободы на срок не более 5 лет или штрафом в размере не более 1 000 000 иен) [14].

В Китае уголовная ответственность за киберпреступления закреплена непосредственно в Уголовном кодексе КНР (далет – УК КНР), что позволяет отнести данное государство к странам с кодифицированной моделью регулирования. Ключевыми являются ст. 285-287[1] УК КНР, посвященные преступлениям в сфере компьютерной информации. Так, ст. 285 УК КНР устанавливает ответственность за незаконное вторжение в компьютерные информационные системы, имеющие отношение к новейшим научно-техническим разработкам, к строительству системы государственной безопасности и государственным делам и наказывается лишением свободы на срок до 3 лет; ст. 286 регулирует ответственность за сокращение (изъятие) текста, исправление, дополнение, создание помех, приведшее к невозможности нормального функционирования компьютерной информационной системы и наказывается лишением свободы до пяти лет, а при особо тяжких последствиях – свыше пяти лет; ст. 287[1] предусматривает ответственность за использование информационных сетей для совершения преступлений, устанавливая наказание в виде лишения свободы до трех лет [10].

Что касается правовой основы для борьбы с киберпреступностью, в Исламской Республике Иран традиционные преступления, совершенные или ставшие возможными благодаря использованию киберпространства, подлежат наказанию в соответствии с исламским Уголовным кодексом.

Важно отметить, что помимо Уголовного кодекса уголовная ответственность за киберпреступления также регулируется специальным Законом о компьютерных преступлениях 2009 г. В частности, в соответствии с этим законом уголовно наказуемыми деяниями были признаны несанкционированный доступ к данным и компьютерным системам, распространение материалов непристойного содержания, осуществление действий, направленных против целостности и конфиденциальности данных, а также хищения и

мошенничество, связанные с использованием компьютеров, данные преступления наказываются штрафом и лишением свободы на срок до 15 лет [12].

В 2025 г. сообщалось, что парламент Ирана утвердил закон об усилении наказания за сотрудничество с враждебными государствами, шпионаж, кибератаки и использование нелицензированных интернет-устройств, в том числе Starlink. согласно ст. 286 Исламского уголовного кодекса, такие действия могут быть признаны «вредительством на земле» и караться смертной казнью [3].

Анализ уголовной ответственности за киберпреступления в законодательстве зарубежных стран позволяет сделать вывод о том, что зарубежные государства выработали различные, но в целом системные подходы к уголовно-правовому противодействию преступлениям в цифровой среде. Общей тенденцией является признание повышенной общественной опасности киберпреступлений, особенно в случаях посягательства на критическую инфраструктуру, государственную безопасность, экономические интересы и конфиденциальность информации. Зарубежный опыт свидетельствует о целесообразности комплексного и системного регулирования киберпреступлений, а также о необходимости четкого разграничения составов преступлений в зависимости от характера посягательства, степени причиненного вреда и объекта уголовно-правовой охраны.

С учетом проведенного анализа представляется возможным сформулировать ряд предложений по совершенствованию уголовного законодательства Российской Федерации:

– учитывая стремительное развитие цифровых технологий и увеличением числа преступлений, совершаемых в сети Интернет, возникает необходимость закрепления на законодательном уровне понятия «киберпреступления» в Уголовном кодексе Российской Федерации. Это позволит систематизировать нормы, регулирующие ответственность за преступления в цифровой сфере;

– уточнить и расширить составы преступлений в сфере компьютерной информации с учетом современных форм киберпреступности (компьютерный шпионаж, атаки на критическую инфраструктуру, незаконный оборот цифровых идентификаторов и доступов;

– предусмотреть самостоятельную уголовную ответственность за подготовительные действия к совершению киберпреступлений;

– в целях усиления защиты национальной безопасности Российской Федерации представляется необходимым введение в Уголовном кодексе Российской Федерации ответственности за военные киберпреступления.

К таким деяниям следует отнести кибератаки, совершаемые в условиях вооруженного конфликта либо направленные против военной информационных систем, систем управления и связи, а также критической инфраструктуры оборонного значения. Целесообразно предусмотреть самостоятельный состав преступления с квалифицирующими признаками за совершение кибератак в интересах иностранного государства, с использованием вредоносного программного обеспечения военного назначения либо повлекших тяжкие последствия. Это позволит обеспечить адекватную уголовно-правовую защиту государства в условиях современных цифровых угроз.

Проведенное исследование показало, что киберпреступления представляют собой одну из наиболее опасных угроз национальной безопасности нашего государства в условиях цифровизации и глобализации. Зарубежные государства используют различные модели уголовно-правового регулирования киберпреступлений, включая нормы уголовных кодексов и специальные законы, при этом прослеживается тенденция к усилению ответственности за посягательства на компьютерную информацию, критическую инфраструктуру и государственную безопасность.

Литература

1. Бурмистрова Ю.В. Соотношение понятий «киберпреступление», «компьютерное преступление» и «преступление в сфере компьютерной информации» // Научные высказывания. 2023. №23 (47). С. 22-25. URL: https://nvjournal.ru/article/SOOTNOShENIE_PONJaTIJ__KIBERPRESTUPLENIE_KOMPJuTERNOE_PRESTUPLENIE_I_PRESTUPLENIE_V_SFERE_KOMPJuTERNOJ_INFORMATsII.
2. Законодательство о киберпреступлениях в зарубежных странах // РИА НОВОСТИ URL: https://ria.ru/20130809/955198703.html (дата обращения 12.02.2026).
3. Интернет был окном в мир. В Иране он стал поводом для тюрьмы и порки // SecurityLab.ru URL: https://www.securitylab.ru/news/560880.php (дата обращения 15.02.2026).
4. Ищенко Е.П. 2015. О криминалистическом обеспечении раскрытия и расследования киберпреступлений. В кн.: Деятельность правоохранительных органов в современных условиях: сборник материалов 20-й международной научно-практической конференции. В 2 томах. Том 1. Иркутск: 336–337.
5. Клишков В.Б., Стебенева Е.В., Яковлева М.А. Киберпреступность: понятие, признаки, основные направления противодействия // Вестник Нижегородского университета им. Н.И. Лобачевского. 2022. № 4. С. 106-114.
6. Компьютерные преступления // BUKH GLOBAL AMERICA'S TOP LAWYERS URL: https://www.bukhglobal.com/ru/ (дата обращения 12.02.2026).
7. Кочкина Э.Л. Определение понятия «киберпреступление». отдельные виды киберпреступлений // Сибирские уголовно-процессуальные и криминалистические чтения. № 3(17). 2017. С. 162-169.
8. Никиташенко В.В. Понятие и признаки киберпреступности // Молодой ученый. — 2021. — № 14 (356). — С. 250-252.
9. Простосердов М.А. 2016. Экономические преступления, совершаемые в киберпространстве, и меры противодействия им. Диссертация кандидата юридических наук. Москва: 232.
10. Уголовный кодекс Китайской Народной Республики // Посольство Китайской Народной Республики в Российской Федерации URL: https://ru.china-embassy.gov.cn/rus/zfhz_0/zgflyd_142850/202504/t20250430_11614090.htm (дата обращения 14.02.2026).
11. Act on Prohibition of Unauthorized Computer Access Act No. 128 of August 13, 1999 // Japanese Law Translation URL: https://www.japaneselawtranslation.go.jp/en/laws/view/3933 (дата обращения 12.02.2026).
12. Islamic Republic of Iran: Computer Crimes Law // IRAN HUMAN RIGHTS Documentation Center URL: https://iranhrdc.org/islamic-republic-of-iran-computer-crimes-law/#chapter_two_%e2%80%93_crimes_against_authenticity_and_integrity_of_data_computer_and_telecommunication_systems (дата обращения 08.03.2026).
13. Jason B. Freeman the Computer Fraud and Abuse Act (CFAA) // FREEMAN|LAW URL: https://freemanlaw.com/computer-fraud-abuse-act-cfaa/ (дата обращения 12.02.2026).
14. Penal Code Act No. 45 of April 24, 1907 // Japanese Law Translation URL: https://www.japaneselawtranslation.go.jp/en/laws/view/3581/en (дата обращения 12.02.2026).
15. Strafgesetzbuch // Bundesamt für Justiz URL: https://www.gesetze-im-internet.de/stgb/index.html (дата обращения 12.02.2026).