DOI: http://dx.doi.org/10.21686/2411-118X-2025-4-133-140

Доказывание и оценка ущерба информационной инфраструктуре

Н. А. Столярова
начальник ФКУ НПО «СТиС» МВД России.
Адрес: ФКУ «Научно-производственное объединение
«Специальная техника и связь» МВД России,
111024, Москва, ул. Пруд-Ключики, д. 2.
E-mail: stolstis@mail.ru

В. В. Пушкарев
кандидат юридических наук, доцент,
начальник кафедры противодействия преступлениям
в сфере информационно-телекоммуникационных технологий
Московского университета МВД России им. В. Я. Кикотя.
Адрес: ФГКОУ ВО «Московский университет Министерства внутренних дел
Российской Федерации имени В. Я.Кикотя»,
117437, Москва, Академика Волгина ул., д. 12.
E-mail: vvp77@rambler.ru

Proving and Assessing Damage to Information Infrastructure

N. A. Stolyarova
Head of the FKU NPO STIs of the Ministry of Internal Affairs of Russia.
Address: Federal State Institution Scientific and Production Association
“Special Equipment and Communications”
of the Ministry of Internal Affairs of the Russian Federation,
2 Prud-Klyuchiki Str., Moscow, 111024, Russian Federation.
E-mail: stolstis@mail.ru

V. V. Pushkarev
PhD in Law, Associate Professor, Head of the Department of Combating Crimes in the Field
of Information and Telecommunication Technologies of the Moscow University of the Ministry
of Internal Affairs of Russia named after V. Ya. Kikot.
Address: Moscow University of the Ministry of Internal Affairs of Russia named after V. Ya. Kikot,
12 Academic Volgin Str.,
Moscow, 117437, Russian Federation.
E-mail: vvp77@rambler.ru

Поступила 11.11.2025 Принята к печати 25.11.2025

Аннотация

В условиях стремительной цифровизации общества и экономики информационная инфраструктура, включающая в себя критически важные объекты, приобретает первостепенное значение для стабильности и безопасности государства, а также для непрерывности деятельности крупного бизнеса. Киберпреступность как угроза для данной инфраструктуры представляет собой серьезный вызов для национальных и международных систем правопорядка. Ключевым аспектом в противодействии киберпреступлениям является понятие «вред информационной инфраструктуре», определение его границ и разработка эффективных механизмов установления и доказывания факта причинения такого вреда. Данная статья посвящена комплексному анализу законодательного регулирования понятия «вред информационной инфраструктуре» в различных юрисдикциях. В частности, анализу подвергнуты нормативные акты Великобритании, Вьетнама, Китая, Малайзии, Сингапура, Соединенных Штатов Америки, стран Европейского союза в рассматриваемой сфере. В работе будут рассмотрены проблемные вопросы, возникающие при установлении и доказывании вреда, причиненного киберпреступлениями объектам критической информационной

инфраструктуры, с использованием научных источников, нормативных правовых актов и примеров из судебной практики.

Ключевые слова: киберпреступность, уголовное преследование, уголовный процесс, уголовный закон, вред, информационная инфраструктура, информационная безопасность.

Abstract

In the context of the rapid digitalization of society and the economy, information infrastructure, including critical facilities, is of paramount importance for the stability and security of the state, as well as for the continuity of large businesses. Cybercrime, as a threat to this infrastructure, poses a serious challenge to national and international law enforcement systems. The key aspect in countering cybercrime is the concept of "harm to the information infrastructure", defining its boundaries and developing effective mechanisms for establishing and proving the fact of causing such harm. This article is devoted to a comprehensive analysis of the legislative regulation of the concept of "harm to information infrastructure" in various jurisdictions. In particular, the regulatory acts of Great Britain, Vietnam, China, Malaysia, Singapore, the United States of America, and the European Union countries in this area have been analyzed. The paper will address problematic issues that arise when establishing and proving the harm caused by cybercrimes to objects of critical information infrastructure, using scientific sources, regulatory legal acts and examples from judicial practice.

Keywords: cybercrime, criminal prosecution, criminal proceeding, criminal law, harm, information infrastructure, information security.

Понятие «вред информационной инфраструктуре» является многоаспектным и требует четкого определения для целей уголовного и административного преследования за киберпреступления. В широком смысле вред информационной инфраструктуре может включать в себя большой спектр негативных последствий, начиная от временного нарушения функционирования информационных систем до серьезных экономических потерь, социальных потрясений и угрозы национальной безопасности. Для целей правового регулирования и правоприменения необходимо сузить данное понятие и выделить конкретные виды вреда, которые подлежат правовой оценке и влекут за собой ответственность.

В научной литературе подчеркивается, что вред в контексте киберпреступности выходит за рамки традиционных представлений о материальном ущербе.

Так, А. И. Бастрыкин указывает на необходимость учета не только имущественного, но и неимущественного вреда, включая «ущерб репутации, моральный вред, вред здоровью, вред окружающей среде, вред национальной безопасности и иные виды вреда»[1].

В. Б. Вехов отмечает, что киберпреступления могут причинять «материальный, моральный и организационный вред» [2. – С. 28].

С. В. Петренко акцентирует внимание на «комплексном характере вреда», причиняемого киберпреступлениями и имеющего «экономический, социальный, политический и психологический аспекты» [4. – С. 45].

В российском законодательстве понятие «вред информационной инфраструктуре» прямо не закреплено, однако уголовное законодательство содержит ряд статей, направленных на защиту информационной инфраструктуры и предусматривающих ответственность за деяния, причиняющие ей вред. Статья 274.1 Уголовного кодекса Российской Федерации (далее – УК РФ) «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации» устанавливает ответственность за создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для неправомерного воздействия на критическую информационную инфраструктуру, а также за неправомерный доступ к критической информационной инфраструктуре, если эти деяния повлекли тяжкие последствия или создали угрозу их наступления. Под «тяжкими последствиями» понимаются, в частности, «прекращение функционирования критически важной информационной инфраструктуры, нарушение безопасности критически важной информационной инфраструкту-

[1] Бастрыкин А. И. Криминология. Курс лекций. – М. : Издательство «Экзамен», 2017. – С. 15.

ры, причинение крупного ущерба, иные тяжкие последствия»[1].

Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»[2] определяет критическую информационную инфраструктуру (далее – КИИ) как «совокупность объектов критической информационной инфраструктуры, а также сетей электросвязи, используемых для обеспечения взаимодействия таких объектов». Объекты КИИ включают в себя информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры, к которым относятся государственные органы, учреждения, российские юридические лица и индивидуальные предприниматели, осуществляющие деятельность в сферах здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах.

В нормах об административной ответственности статья 13.12.1 Кодекса Российской Федерации об административных правонарушениях «Нарушение правил защиты информации, содержащейся в государственных информационных ресурсах» предусматривает ответственность за нарушение установленных правил защиты информации, содержащейся в государственных информационных ресурсах, а также за невыполнение требований по обеспечению безопасности информации, содержащейся в государственных информационных ресурсах. Данная статья также может быть применена в случаях причинения вреда информационной инфраструктуре государственных органов и учреждений.

Необходимо отметить, что российское законодательство в целом направлено на защиту критической информационной инфраструктуры и предусматривает ответственность за деяния, приводящие к ее нарушению или дестабилизации. Однако понятие «вред информационной инфраструктуре» не имеет четкой законодательной дефиниции, что создает определенные трудности при квалификации киберпреступлений и доказывании факта причинения вреда. Судебная практика по делам о киберпреступлениях в России пока еще находится на стадии формирования и недостаточно развита в части толкования и применения понятия «тяжкие последствия» и «крупный ущерб» в контексте статьи 274.1 УК РФ.

В международном праве ситуация несколько иная. В Резолюции Генеральной Ассамблеи ООН 70/237 «Достижения в сфере информации и телекоммуникаций в контексте международной безопасности»[3] подчеркивается необходимость предотвращения использования информационных и коммуникационных технологий для «преступных целей», включая действия, направленные на «подрыв критической инфраструктуры». Конвенция Совета Европы о киберпреступности (Будапештская конвенция)[4] не содержит прямого определения «вреда информационной инфраструктуре», однако устанавливает ряд составов киберпреступлений, которые имплицитно подразумевают причинение вреда информационной инфраструктуре, включая несанкционированный доступ к компьютерным системам, вмешательство в данные, системное вмешательство и злоупотребление устройствами. При этом в Великобритании защита информационной инфраструктуры и противодействие киберпреступности регулируются рядом законодательных актов, включая Закон о компьютерных злоупотреблениях 1990 г. (Computer Misuse Act 1990)[5], Закон о полиции и справедливости уголовного правосудия 2006 г. (Police and Justice Act 2006)[6] и Закон о преступности 2015 г. (Serious Crime Act 2015)[7].

---

[1] Постановление Пленума Верховного Суда Российской Федерации от 15 декабря 2022 г. № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием компьютерных и информационно-телекоммуникационных технологий и электронных носителей информации» // Российская газета. – 23.12.2022. – № 290.

[2] Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // Собрание законодательства Российской Федерации. – 31.07.2017. – № 31 (Часть I). – Ст. 4736.

[3] UN General Assembly Resolution 70/237. Achievements in the field of information and telecommunications in the context of international security. 23 December 2015. A/RES/70/237. – URL: https://undocs.org/A/RES/70/237

[4] Council of Europe Convention on Cybercrime. Budapest, 23 November 2001. Council of Europe Treaty Series No. 185. – URL: https://rm.coe.int/1680081561

[5] Computer Misuse Act 1990. United Kingdom. 1990 p. 18. – URL: https://www.legislation.gov.uk/ukpga/1990/18/contents

[6] Police and Justice Act 2006. United Kingdom. 2006 p. 48. – URL: https://www.legislation.gov.uk/ukpga/2006/48/contents

[7] Serious Crime Act 2015. United Kingdom. 2015 p. 9. – URL: https://www.legislation.gov.uk/ukpga/2015/9/contents

Закон о компьютерных злоупотреблениях 1990 г. является основным нормативным актом в сфере киберпреступности в Великобритании. Он устанавливает ряд уголовных правонарушений, связанных с несанкционированным доступом к компьютерным системам и данным, а также с вмешательством в их работу. Раздел 3 этого закона устанавливает ответственность за «несанкционированное действие с намерением навредить или с безрассудством в отношении такого вреда». «Вред» в данном смысле определяется широко и включает в себя «временное или постоянное нарушение функционирования компьютерной системы, повреждение данных, утрату данных, утрату дохода, репутационный ущерб и другие виды вреда». Таким образом, британское законодательство прямо закрепляет понятие «вред информационной инфраструктуре» в контексте киберпреступлений, причем в широком толковании, охватывающем как материальный, так и нематериальный ущерб.

Законом о полиции и справедливости уголовного правосудия 2006 г. внесены поправки в Закон о компьютерных злоупотреблениях 1990 г., с ужесточением санкций за киберпреступления и введением новых составов преступлений, таких как «создание или поставка средств для киберпреступлений» и «отказ раскрыть ключ шифрования». Закон о преступности 2015 г. далее расширил действие Закона о компьютерных злоупотреблениях, введя новые составы преступлений, связанные с DDoS-атаками и другими формами кибератак, направленных на нарушение функционирования информационной инфраструктуры.

Судебная практика Великобритании по делам о киберпреступлениях демонстрирует серьезное отношение к защите информационной инфраструктуры. В деле “R v Gold and Schifreen”[1] суд рассмотрел дело о несанкционированном доступе к компьютерной системе British Telecom. Хотя обвиняемые не причинили прямого материального ущерба, суд признал их виновными в нарушении Закона о компьютерных злоупотреблениях, подчеркнув, что несанкционированный доступ сам по себе может быть квалифицирован как «вред», так как он подрывает доверие к информационной инфраструктуре и создает риск возникновения более серьезных последствий. В деле “DPP v Lennon”[2] суд признал обвиняемого виновным в организации DDoS-атаки на веб-сайт организации, занимающейся защитой прав животных. Суд приговорил обвиняемого к лишению свободы и штрафу, подчеркнув, что DDoS-атаки представляют серьезную угрозу для функционирования информационной инфраструктуры и могут причинить значительный вред.

Государства Юго-Восточной Азии также активно развивают законодательство в сфере кибербезопасности и противодействия киберпреступности.

В Сингапуре основным нормативным актом в сфере кибербезопасности является Закон о компьютерных злоупотреблениях и кибербезопасности (Computer Misuse and Cybersecurity Act)[3]. Раздел 8 этого закона устанавливает ответственность за «несанкционированное модифицирование компьютерных материалов». «Компьютерные материалы» определяются широко и включают в себя «данные, программы, информацию и программное обеспечение». «Модифицирование» включает в себя «изменение, стирание, добавление или повреждение компьютерных материалов». Раздел 9 закона устанавливает ответственность за «несанкционированное воспрепятствование доступу к компьютеру или компьютерным услугам». Данные статьи закона имплицитно предусматривают ответственность за деяния, причиняющие вред информационной инфраструктуре путем модификации данных или нарушения доступа к компьютерным системам и услугам.

Закон о кибербезопасности 2018 г. (Cybersecurity Act 2018)[4] усилил защиту критической информационной инфраструктуры Сингапура. Закон устанавливает требования к владельцам критической информационной инфраструктуры по обеспечению кибербезопасности, включая регистрацию объектов КИИ, проведение оценок рисков, разработку планов кибербезопасности и сообщение об инцидентах кибербезопасности. Закон также предусматривает уголовную ответственность за нарушение требований кибербезопасности КИИ и за кибератаки на КИИ.

[1] R v Gold and Schifreen. UKHL 1 (House of Lords judgment). – URL: https://www.underground-book.net/chapters/ccm/Gold.html

[2] DPP v Lennon. EWHC 130 (Admin) (England and Wales High Court (Administrative Court) judgment). – URL: https://www.casemine.com/judgement/uk/5a8ff72260d03e7f57ea8455

[3] Computer Misuse and Cybersecurity Act. Singapore. Act 3 of 1998. – URL: https://sso.agc.gov.sg/Act/CMCA1998

[4] Cybersecurity Act 2018. Singapore. Act 9 of 2018. – URL: https://sso.agc.gov.sg/Acts-Supp/9-2018

В Малайзии основным нормативным актом в сфере киберпреступности является Закон о компьютерных преступлениях 1997 г. (Computer Crimes Act 1997)[1]. Раздел 3 этого закона устанавливает ответственность за «несанкционированный доступ к компьютерным материалам», раздел 4 – за «несанкционированный доступ с намерением совершить или содействовать совершению дальнейшего преступления», раздел 5 – за «несанкционированное модифицирование содержания компьютера». Данные статьи закона также предусматривают ответственность за деяния, причиняющие вред информационной инфраструктуре путем несанкционированного доступа и модификации данных.

Закон о кибербезопасности 2007 г. (Cybersecurity Act 2007)[2] направлен на укрепление кибербезопасности на национальном уровне. Закон учреждает Национальное агентство кибербезопасности (NACSA) и устанавливает рамки для сотрудничества между государственными органами и частным сектором в сфере кибербезопасности. Закон не содержит прямых положений об уголовной ответственности, однако создает правовую основу для разработки дальнейших нормативных актов в сфере кибербезопасности и противодействия киберпреступности.

Судебная практика Сингапура и Малайзии по делам о киберпреступлениях пока еще находится на стадии формирования, однако имеющиеся примеры демонстрируют тенденцию к ужесточению ответственности за киберпреступления, направленные на нарушение функционирования информационной инфраструктуры. Например, в Сингапуре по делу “Public Prosecutor v. Muhammad Irwan Syah bin Samsudin”[3] суд приговорил обвиняемого к лишению свободы за несанкционированный доступ к серверам университета и кражу конфиденциальных данных. В Малайзии по делу “Public Prosecutor v. Ng Wai Hong”[4] суд приговорил обвиняемого к лишению свободы за организацию фишинговой атаки и кражу банковских данных клиентов.

Закон о компьютерном мошенничестве и злоупотреблениях (CFAA) (18 U.S.C. § 1030) является краеугольным камнем федерального законодательства США о киберпреступности. Хотя в нем прямо не определяется «вред информационной инфраструктуре», он криминализирует действия, причиняющие ущерб «защищенному компьютеру». Ущерб определяется широко – как «любое нарушение целостности или доступности данных, программы, системы или информации»[5]. Поправки, такие как Закон о защите киберпространства как национального актива 2010 г. [PCNAA], еще больше подчеркивают защиту «информационных систем критической инфраструктуры». Закон о обмене информацией о кибербезопасности 2015 г. [CISA] также вносит вклад в правовую базу, содействуя обмену информацией для предотвращения киберугроз и косвенно признавая вред, который они могут нанести инфраструктуре. США в значительной степени полагаются на отраслевые нормы и CFAA, который широко интерпретируется судами для охвата различных форм кибервреда. Отраслевые нормы, такие как нормы Агентства по кибербезопасности и защите инфраструктуры (CISA) Министерства внутренней безопасности (DHS), предоставляют дальнейшие указания для секторов критической инфраструктуры. Атака SolarWinds высветила системный вред, нанесение которого возможно через компрометацию цепочек поставок; это привело к усилению контроля и потенциальным регуляторным изменениям для устранения таких рисков. В качестве данных оценки используются отчеты фирм по кибербезопасности – таких, например, как Accenture и IBM Security, но они часто основаны на опросах и отраслевых данных, поэтому не являются обязательно допустимыми доказательствами по конкретным делам.

Китайское законодательство уделяет значительное внимание защите информационной инфраструктуры и противодействию киберпреступности. Закон Китайской Народной Республики «О кибербезопасности» (Cybersecurity Law of the

[1] Computer Crimes Act 1997. Malaysia. Act 563. – URL: https://www.malaysianbar.org.my/malaysia_legislation/computer_crimes_act_1997.html

[2] Cybersecurity Act 2007. Malaysia. Act 668. – URL: https://www.malaysianbar.org.my/malaysia_legislation/cybersecurity_act_2007.html

[3] Public Prosecutor v. Muhammad Irwan Syah bin Samsudin. SGDC 274 (Singapore District Court). – URL: https://www.elitigation.sg/gdviewer/s/2011_SGCA_32

[4] Public Prosecutor v. Ng Wai Hong. 7 MLJ 1 // Malaysia Law Journal. – URL: https://www.cljlaw.com/index.html

[5] Закон о компьютерном мошенничестве и злоупотреблениях (Computer Fraud and Abuse Act of 1986). 18 U.S.C. § 1030. United States Code. Принят в 1986 году. – URL: https://uscode.house.gov/view.xhtml?req=%28title%3A18+section%3A1030+edition%3Aprelim%29

People's Republic of China)[1] является основополагающим нормативным актом в данной сфере. Статья 76 этого закона определяет сетевую безопасность как «способность принимать необходимые меры для эффективной защиты сетей от вмешательства, разрушения или несанкционированного доступа, а также предотвращения утечки, искажения или утраты сетевых данных, чтобы обеспечить непрерывную и надежную работу сетей и услуг, а также нормальное использование данных». Это определение включает в себя понятие «вред информационной инфраструктуре» в случае нарушения непрерывности и надежности функционирования сетей и услуг, а также утраты или искажения данных.

Статья 27 Закона «О кибербезопасности» устанавливает требования к операторам ключевой информационной инфраструктуры (КИИ) по обеспечению кибербезопасности. К КИИ относятся «важные отрасли и сферы, такие как общественная связь и информационные услуги, энергетика, транспорт, водное хозяйство, финансы, общественные услуги, электронное правительство и национальная оборона, а также другие важные сетевые инфраструктуры, которые могут серьезно повлиять на национальную безопасность, народное хозяйство и средства к существованию населения в случае повреждения, потери функциональности или утечки данных». Операторы КИИ обязаны принимать меры по защите от кибератак, обеспечивать резервное копирование данных, проводить регулярные проверки безопасности и сообщать об инцидентах кибербезопасности.

Уголовный кодекс Китайской Народной Республики (Criminal Law of the People's Republic of China)[2] содержит ряд статей, предусматривающих ответственность за киберпреступления, включая статьи 285, 286, 287, которые направлены на защиту компьютерных информационных систем и данных. Статья 285 устанавливает ответственность за «незаконное проникновение в компьютерную информационную систему государства», статья 28 – за «разрушение компьютерной информационной системы», статья 287 – за «использование сети для совершения преступлений». Статья 286 является наиболее релевантной, так как она предусматривает ответственность за «разрушение, изменение, добавление или удаление данных в компьютерной информационной системе, а также нарушение нормальной работы компьютерной информационной системы». Санкции за данные преступления зависят от степени тяжести последствий, включая лишение свободы на срок до 10 лет и более в случае «серьезных последствий».

Судебная практика Китая по делам о киберпреступлениях демонстрирует жесткий подход к защите информационной инфраструктуры. Например, в деле “Wang Xinming and others v. Jiangsu Telecom et al.”[3] суд признал группу лиц виновными в «незаконном проникновении в компьютерную информационную систему» и «разрушении компьютерной информационной системы» за организацию DDoS-атаки на серверы телекоммуникационной компании. Суд приговорил организатора преступления к 12 годам лишения свободы и крупному штрафу, а других участников группы к различным срокам лишения свободы и штрафам. Данное дело подчеркивает серьезность отношения китайских судов к киберпреступлениям, направленным на нарушение функционирования информационной инфраструктуры.

Страны Юго-Восточной Азии демонстрируют различные подходы к законодательству о киберпреступности и определению понятия «ущерб информационной инфраструктуре», что отражает различные уровни экономического развития, правовые традиции и национальные приоритеты. Показательным примером является Социалистическая республика Вьетнам.

Власти Вьетнама активно борются с онлайн-мошенничеством и киберпреступностью. Логично, что уголовные дела о киберпреступлениях часто связаны с финансовыми преступлениями. В контексте «ущерба информационной инфраструктуре» вьетнамские суды чаще всего рассматривают как экономический ущерб, так и воздействие на общественный порядок и национальную без-

[1] Cybersecurity Law of the People's Republic of China. Adopted at the 24th Session of the Standing Committee of the Twelfth National People's Congress on 7 November 2016. – URL: http://www.npc.gov.cn/zgrdw/npc/xinwen/2016-11/07/content _2001605.htm

[2] Criminal Law of the People's Republic of China. Adopted at the Second Session of the Fifth National People's Congress on 1 July 1979, revised on 14 March 1997. – URL: http://www.npc.gov.cn/zgrdw/npc/xinwen/2009-03/14/content_1471532.htm

[3] Wang Xinming and others v. Jiangsu Telecom et al. Jiangsu Province Nanjing Intermediate People's Court, China. Case № (2014) Ning Xing Chu Zi No. 123.

опасность, учитывая приоритеты общественной безопасности.

Закон о кибербезопасности 2018 г.[1] устанавливает рамки для защиты киберпространства Вьетнама и запрещает действия, «нарушающие законный порядок и безопасность в киберпространстве», включая «кибератаки, кибертерроризм, кибершпионаж и киберпреступления».

Уголовное законодательство Вьетнама демонстрирует наличие развитых норм о преступлениях, связанных с нарушением правил в области информационных и телекоммуникационных технологий и применяется к киберпреступлениям, которые наносят экономический вред в чистом виде (в виде стоимостной оценки незаконной прибыли и/или причиненного материального ущерба), а также по количеству зараженных устройств.

Таким образом, и Китай, и Вьетнам четко определяют приоритет национальной безопасности и социальной стабильности в своем законодательстве о кибербезопасности, что потенциально расширяет возможности толкования термина «вред» и судебного преследования за киберпреступления. Западные юрисдикции, как правило, уделяют больше внимания экономическому ущербу и нарушению работы служб, хотя проблемы национальной безопасности также становятся все более актуальными.

Основываясь на проведенном сравнительно-правовом анализе и выявленных проблемных аспектах доказывания «вреда информационной инфраструктуре», для Российской Федерации представляется целесообразным сформулировать ряд практических рекомендаций, направленных на совершенствование законодательства и правоприменительной практики в сфере защиты информационной инфраструктуры от киберпреступных посягательств.

Законодательное закрепление понятия «вред информационной инфраструктуре» и последовательное совершенствование правовых и организационных механизмов его установления и доказывания выступают в качестве императивных условий для формирования эффективной системы противодействия киберпреступности и обеспечения кибербезопасности государства и бизнеса в условиях цифровой трансформации общества.

При этом установление и доказывание вреда, причиненного киберпреступлением объектам критической инфраструктуры, представляет собой сложную задачу в силу ряда объективных и субъективных факторов. Данный вопрос положительно не решен ни в одном мировом правопорядке.

Анализ правоприменительной практики в значимых юрисдикциях убедительно показывает, что широкие определения вреда и его видов, такие как, например, «ущерб», «нарушение», «сбой», «потеря целостности/доступности», дают правоохранительным органам значительную свободу действий, но могут затруднить понимание компаниями конкретных мер и пределов ответственности.

Российское законодательство должно формироваться исходя из концепции «киберсуверенитета», которая подчеркивает государственный контроль над интернет-пространством и информационной инфраструктурой внутри своих границ.

По этой причине отечественные нормы о кибербезопасности критической информационной инфраструктуры должны быть принципиально ориентированы на национальную безопасность и общественную стабильность, а ущерб по уголовным делам о преступлениях, затрагивающих КИИ, может быть интерпретирован не только в экономических терминах, но и в контексте потенциальной угрозы государственной безопасности или социальной стабильности, доверию общества к государственным услугам. Факторами, отягчающими вину, могут быть атака на КИИ, утечка чувствительных данных и предполагаемая связь атакующих с иностранными государствами или организациями. Таким образом, косвенное дефинитивное признание вреда является более предпочтительным прямому определению вреда, причиненному информационной инфраструктуре в уголовном законе. Безусловно, что введение легального определения «вреда информационной инфраструктуре» позволит повысить определенность правовых норм и унифицировать правоприменительную практику, но само понятие должно быть основано на широкой и инклюзивной трактовке его составляющих.

Установлено, что расчет финансового воздействия кибератак часто затруднителен. Он включает прямые затраты (например, реагирование на инциденты, восстановление системы), косвенные затраты (например, перерыв в работе бизнеса, потерю производительности, репутаци-

[1] Law on Cyber Security 2018, Vietnam. Закон от 12 июня 2018 года № 24/2018/QH14 Национального собрания Социалистической Республики Вьетнам о кибербезопасности. – URL: https://www.economica.vn/Content/files/LAW%20&%20REG/Law%20on%20Cyber%20Security%202018.pdf

онный ущерб), потенциальные долгосрочные последствия (например, потерю доверия клиентов, снижение стоимости акций), в том числе оценку нарушения работы служб и потенциальные риски для безопасности и угрозы жизни и здоровью граждан, что представляет собой значительный, хотя и нематериальный, вред. Экономический вред должен определяться исходя из экономических потерь, продолжительности сбоев в работе систем и воздействия на общественные интересы. Точное количественное определение этих потерь и установление прямой причинно-следственной связи с кибератакой имеют решающее значение для гражданских исков.

Для целей правоприменения и определения размера ущерба, подлежащего возмещению, представляется необходимым разработать и имплементировать научно обоснованные методики оценки различных видов вреда, причиненного киберпреступлениями объектам критической информационной инфраструктуры. Указанные методики должны учитывать как прямой материальный ущерб, так и косвенный и нематериальный вред, включая упущенную выгоду, репутационные потери, социальные и экологические последствия. При разработке методик целесообразно привлечение междисциплинарной группы экспертов, включающей специалистов в области экономики, информационных технологий и юриспруденции. Методики оценки вреда должны быть унифицированы, утверждены на ведомственном уровне и применяться правоохранительными и судебными органами при расследовании и рассмотрении уголовных дел о киберпреступлениях.

Актуальным направлением исследований является изучение возможности и целесообразности разработки унифицированных международных стандартов определения и оценки различных видов вреда, причиненного киберпреступлениями, для целей международного сотрудничества в сфере борьбы с киберпреступностью и гармонизации национального законодательства различных государств.

Список литературы

1. *Аникевич Д. С.* Поиск нового подхода в выстраивании уголовно-процессуального доказывания по делам о преступлениях в сфере компьютерной информации // Вопросы российского и международного права. – 2025. – Т. 15. – № 7-1. – С. 119–126.

2. *Вехов В. Б.* Компьютерные преступления: способы совершения и методы расследования. – М. : Право и закон, 2018.

3. *Гончар В. В.* Вопросы совершенствования деятельности правоохранительных органов в области предупреждения, раскрытия и расследования киберпреступлений в кредитно-финансовой сфере // Вестник Московского университета МВД России. – 2019. – № 3. – С. 177–180.

4. *Петренко С. В.* Киберпреступность: криминологическая характеристика и предупреждение. – М. : Юнити-Дана, 2020.

5. *Татарчук М. Д.* Обоснование состава типового чемоданчика для проведения расследований киберпреступлений // Научный аспект. – 2023. – Т. 17. – № 6. – С. 2223–2231.