КОМПАРАТИВИСТСКИЕ ИССЛЕДОВАНИЯ УГОЛОВНОГО ПРАВА, КРИМИНОЛОГИИ И УГОЛОВНО-ИСПОЛНИТЕЛЬНОГО ПРАВА

КОМПЬЮТЕРНАЯ ИНФОРМАЦИЯ КАК ПРЕДМЕТ ПОСЯГАТЕЛЬСТВА ПРИ НЕПРАВОМЕРНОМ ДОСТУПЕ: СРАВНИТЕЛЬНЫЙ АНАЛИЗ ЗАКОНОДАТЕЛЬСТВА США И РОССИИ*

ДРЕМЛЮГА Роман Игоревич, доцент Юридической школы Дальневосточного федерального университета, кандидат юридических наук

690091, Россия, г. Владивосток, ул. Суханова, 8

E-mail: dreamluck@yandex.ru

Рассматриваются действующие нормы федерального уголовного законодательства и законодательства штатов, устанавливающие уголовную ответственность за преступления в сфере неправомерного доступа к компьютерной информации. Акцент сделан на предмет преступного посягательства — компьютерную информацию. Автор анализирует категории компьютерной информации, за доступ к которой установлена уголовная ответственность в США. Помимо рассмотрения конкретных уголовно-правовых норм, приводятся материалы судебной практики США и России.

Автор приходит к выводу, что законодательство и практика правоприменения в США зачастую учитывают свойства и характеристики самой информации, к которой осуществляется неправомерный доступ. Свойства информации для американского законодателя и правоприменителя отражают общественную опасность преступлений в сфере компьютерной информации. В российской практике на квалификацию неправомерного доступа к охраняемой законом информации в первую очередь влияют негативные последствия деяния или характеристики субъекта. Такая практика соответствует парадигме традиционной (доцифровой) экономики, где информация является лишь средством осуществления общественных отношений или государственного управления. При заявленном общегосударственном переходе к цифровой экономике, когда информация — это основная ценность и продукт хозяйственной деятельности, российскому законодателю и правоприменителю придется пересмотреть существующие подходы. Именно свойства и характеристики информации, к которой осуществляется преступный неправомерный доступ, должны стать квалифицирующими признаками для преступлений такого рода.

Ключевые слова: компьютерная информация, компьютерные преступления, уголовное право США, преступления в сфере компьютерной информации.

COMPUTER INFORMATION AS AN TARGET FOR ILLEGAL ACCESS: COMPARATIVE ANALYSIS OF THE USA AND RUSSIAN LEGISLATION

R. I. DREMLYUGA, associate professor at the School of Law of the Far Eastern Federal University, candidate of legal sciences
8, Sukhanov st., Vladivostok, Russia, 690091

E-mail: dreamluck@yandex.ru

The proposed article deals with the current norms of the federal criminal law of the United States of America and state-level legislation that criminalize crimes in the field of unauthorized access to computer information. The emphasis in the article is on the subject of criminal assault: computer information. The author analyzes the categories of computer information for which criminal responsibility is established in the United States. In addition to reviewing specific criminal law norms, the article presents materials of judicial practice of both the US and the Russian Federation on the topic of the research.

The author of this study concludes that the law and court practice in the United States of America often takes into account the properties and characteristics of the illegally accessed information itself. The properties of information for the American legislator and law enforcer reflect the social danger of computer crimes. In Russian practice, the qualification of illegal access to information, in the first place, is affected by the negative consequences of the act or characteristics of the offender. This practice corresponds to the paradigm of the traditional (pre-digital) economy, where information is only a means of implementing public relations or relations with government. In accordance with the declared nation-wide transition to a digital economy, where information is the main value and product of economic activity, the Russian legislator and law enforcement officer have to reconsider existing

* Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 18-29-16129.

approaches. The properties and characteristics of information that is object to criminal unlawful access should become qualifying factors for such kind of crimes.

Keywords: computer information, computer crimes, the criminal law of the United States, crimes in the sphere of computer information.

DOI: 10.12737/art.2018.6.14

Значимость развития в России сектора цифровой экономики бесспорна, этот тезис в очередной раз подчеркнул Президент Российской Федерации В. В. Путин в выступлении на Петербургском международном экономическом форуме¹. Развитие цифровой экономики в любом государстве мира подразумевает внедрение новых подходов в регулирование общественных отношений, связанных с оборотом компьютерной информации². Одним из основных элементов российской государственной политики по созданию необходимых условий для развития цифровой экономики является обеспечение информационной безопасности³. Мировая практика доказывает, что с ростом «цифровизации» экономики возрастает роль защиты публичной и частной компьютерной информации от преступных посягательств.

Как отмечено в программных документах, «цифровая экономика представляет собой хозяйственную деятельность, ключевым фактором производства в которой являются данные в цифровой форме»⁴. Понятия «данные в цифровой форме», используемое в программе «Цифровая экономика», и «компьютерная информация», сформулированное в Уголовном кодексе РФ, сходны по смыслу⁵. Это свидетельствует о повышении значимости применения уголовного закона в сфере охраны компьютерной информации.

В глобальном масштабе наиболее «унифицированным» преступным деянием в сфере компьютерной информации является неправомерный доступ к компьютерной информации. Так, согласно исследованию Управления ООН по наркотикам и преступно-

сти, неправомерный доступ (англ. Illegal access) является уголовным преступлением в 93% стран мира⁶. Несмотря на повсеместную унификацию указанной нормы, предметом такого рода посягательств может выступать различающаяся по своим юридическим и физическим свойствам компьютерная информация.

В отдельных странах цифровая экономика уже сейчас занимает значительную долю валового внутреннего продукта (ВВП). Анализируя нормы уголовного законодательства и практику правоприменения в сфере уголовно-правовой охраны компьютерной информации таких стран, можно спрогнозировать пути развития отечественного уголовного закона и выявить варианты его модернизации. Сравнительное исследование нормативной базы и правоприменения в области уголовно-правовой охраны компьютерной информации позволяет лучше понять существующие затруднения, ошибки в квалификации и найти пути их устранения.

Мировым лидером в области цифровой экономики остаются Соединенные Штаты Америки⁷. В США была разработана сеть Интернет и приняты первые законы, предусматривающие уголовную ответственность за преступления в сфере компьютерной информации. В связи с этим анализ законов и практики правоприменения США в указанной сфере представляется особо результативным.

Все преступления в США подразделяются на федеральные (federal crimes), ответственность за совершение которых предусмотрена федеральным законодательством, и преступления, за которые ответственность установлена законодательством отдельных штатов (state crimes)⁸. То есть в США уголовное законодательство разрознено — помимо системы федерального уголовного законодательства здесь действуют 52 самостоятельные системы: 51 штат и федеральный округ Колумбия, где расположена столица страны. Каждый штат чаще всего имеет свой свод уголовного законодательства, которое может отличаться по формулировкам, признакам состава и санкциям.

В российском уголовном законе, который регламентирует ответственность за неправомерный до-

¹ Владимир Путин: Внедрить цифровые технологии во все сферы жизни. URL: <https://rg.ru/2017/06/04/reg-szfo/vladimir-putin-vnedrit-cifrovye-tehnologii-vo-vse-sfery-zhizni.html>.

² См.: Linkov I., Trump B. D., Poinatte-Jones K. Governance Strategies for a Sustainable Digital World // Sustainability (Switzerland). 2018. Vol. 10. Iss. 2. URL: <http://www.mdpi.com/2071-1050/10/2/440/htm>; Ali M. A., Hoque M. R., Alam K. An Empirical Investigation of the Relationship Between E-Government Development and the Digital Economy: the Case of Asian Countries // Journal of Knowledge Management, 2018. Vol. 22. Iss. 5. URL: <https://www.emeraldinsight.com/doi/abs/10.1108/JKM-10-2017-0477>.

³ См. распоряжение Правительства РФ от 28 июля 2017 г. № 1632-р «Об утверждении программы “Цифровая экономика Российской Федерации”».

⁴ Там же.

⁵ См., например: Дремлюга Р. И. Понятие «компьютерная информация»: спорные вопросы в теории и законе // Библиотека уголовного права и криминологии. 2018. № 1. С. 108—115.

⁶ См.: Comprehensive Study on Cybercrime. URL: http://www.unodc.org/documents/organized-crime/cybercrime/CYBERCRIME_STUDY_210213.pdf.

⁷ См.: Digital Economy. URL: <https://www.commerce.gov/tags/digital-economy>.

⁸ См.: Брославский Л. И. Уголовная ответственность за экологические преступления в области охраны вод в США // Журнал российского права. 2008. № 3. С. 124.

ступ к компьютерной информации, охраняемая законом информация на подвиды не разделена. Законодатель США, в свою очередь, устанавливает уголовную ответственность за неправомерный доступ к компьютерной информации в зависимости от ее характеристик. Уголовные нормы, устанавливающие уголовную ответственность за незаконный доступ к компьютерной информации, содержатся в ст. 1030 «Мошенничество и связанные с ним действия на компьютере» (Fraud and related activity in connection with computers) Закона федерального уровня по борьбе с компьютерным мошенничеством и злоупотреблениями (The Computer Fraud and Abuse Act)⁹.

Часть 1(a) ст. 1030 в качестве предмета рассматривает информацию, неправомерное раскрытие которой угрожает национальной безопасности или международным отношениям, а также информацию, указанную в § «у» секции 11 Закона об атомной энергии¹⁰.

В части 1(b) ст. 1030 предметом выступает информация, которая содержится в записях финансовых институтов или организаций, выпускающих платежные карты (information contained in a financial record of a financial institution, or of a card issuer) или находится в файлах докладов о потребителях, указанных в Законе о честной кредитной отчетности (contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act).

Часть 1(c) ст. 1030 рассматривает в качестве предмета информацию на любых компьютерах правительственных организаций или на компьютерах, используемых для нужд таких организаций. Если понимать буквально, то данная норма рассматривает в качестве предмета техническое устройство — компьютер, а не его данные — компьютерную информацию.

Закон по борьбе с компьютерным мошенничеством и злоупотреблением не охватывает неавторизованный доступ к любой персональной информации, режим обращения с которой установил ее владелец. Так как упомянутый Закон является федеральным, он охватывает только федеральные преступления (federal felony)¹¹ и обеспечивает уголовно-правовую охрану только определенных видов информации. Нормы Закона охватывают только посягательства на наиболее значимые для общества и государства виды информации. Другие ее виды яв-

ляются предметом преступлений согласно законодательству штатов.

Например, в штате Вирджиния применяется Закон о компьютерных преступлениях (The Virginia Computer Crimes Act). Несмотря на то что акт преимущественно содержит уголовно-правовые нормы, в нем также есть нормы гражданско-правового характера, например, связанные с подачей иска по возмещению вреда, вызванного неправомерным доступом¹². Приведенный статут устанавливает уголовную ответственность за доступ к любой информации без наличия прав на это, перечисляя среди прочих видов данных: кредитные, персональные или о доходах. То есть пробел в федеральном уголовном законодательстве США устраняется на уровне законодательства штата.

Другим примером того, что частная информация охраняется уголовным законом, является Калифорнийский закон, охватывающий доступ к компьютерным данным и мошеннические действия (California Comprehensive Computer Data Access and Fraud Act)¹³. Данный нормативный акт не является самостоятельным, а включен как раздел в Уголовный кодекс штата Калифорния (дословно — Кодекс о наказаниях — California Penal Code). Как указано в тексте акта, его цель — расширить степень защиты физических лиц, бизнеса и правительственных организаций от вмешательства, повреждения и несанкционированного доступа к законно созданной компьютерной информации и компьютерным системам (expand the degree of protection afforded to individuals, businesses, and governmental agencies from tampering, interference, damage, and unauthorized access to lawfully created computer data and computer systems). Например, ч. 4(c) ст. 502 устанавливает уголовную ответственность¹⁴ за доступ с косвенным умыслом без прав на это действие, сопровождаемый добавлением, изменением, повреждением, удалением или разрушением *любой* компьютерной информации (данных), программного обеспечения (knowingly accesses and without permission adds, alters, damages, deletes, or destroys *any* data, computer software, or computer programs).

Кодекс наказаний штата Техас также устанавливает уголовную ответственность за неправомерный доступ к компьютерной информации¹⁵. Статья 33.02

¹² См.: Virginia Computer Crimes Act, Virginia Code Section 18.2-152.1 et seq. of 11 April 1984. URL: <https://law.lis.virginia.gov/vacode/title18.2/chapter5/section18.2-152.1/>.

¹³ California Comprehensive Computer Data Access and Fraud Act (California Computer Act), California Penal Code § 502. URL: https://leginfo.ca.gov/faces/codes_displaySection.xhtml?lawCode=PEN§ionNum=502.

¹⁴ Часть 1(d) определяет, что это правонарушение относится к преступлениям.

¹⁵ См.: Texas Penal Code. URL: <http://www.statutes.legis.state.tx.us/Docs/PE/pdf/PE.33.pdf>.

⁹ URL: <https://www.energy.gov/sites/prod/files/cioproducts/ComputerFraud-AbuseAct.pdf>.

¹⁰ Речь об информации о разработке, производстве и утилизации ядерного оружия и материалов. URL: <https://www.nrc.gov/docs/ML1327/ML13274A489.pdf>.

¹¹ См.: Kerr O. S. Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes // New York University Law Review. 2003. Vol. 78. P. 1661.

«Нарушение компьютерной безопасности» регламентирует уголовную ответственность за доступ к компьютеру, компьютерной системе или сети без согласия владельца. Тяжесть преступного деяния определяется в зависимости от того, к какой информации осуществлен доступ. Так, преступление, направленное на правительственные структуры и критически важные инфраструктурные объекты, признается тяжким преступлением (felony) ст. 33.02 (b)(2), а все остальные категории неправомерного доступа — деянием небольшой и средней тяжести (misdemeanor) ст. 33.02 (b). В данном случае предметом выступает не только компьютерная информация, но и сам компьютер, это позволяет признать преступным не только проникновение и повреждение информации «цифровыми» методами. То есть повреждение критического узла информационной инфраструктуры посредством, например, топора будет также квалифицировано по данной статье.

Анализ федерального законодательства и уголовно-правовых норм отдельных штатов Америки показывает, что предметом выступает как информация, защищенная законом, например государственная тайна или коммерческая тайна, так и информация, режим доступа к которой определил пользователь. В свою очередь, уголовная ответственность за несанкционированный доступ к первой категории информации закреплена на федеральном уровне, а ко второй — в правовых актах штата.

Информация как предмет влияет на квалификацию и наказание, т. е. отражает общественную опасность преступного деяния. Соединенные Штаты Америки являются одним из флагманов перехода к цифровому обществу и цифровой экономике, поэтому законодательство отражает значимость информации и ее свойств.

Показательным является дело «США против А. Шварца», который, получив доступ к электронному ресурсу по хранению научных статей Массачусетского технологического института (МТИ), незаконно их скопировал и распространил. Ему было предъявлено несколько обвинений, в том числе в незаконном доступе¹⁶. МТИ отказался от обвинений, и скопированные статьи были в общем доступе бесплатно для любого посетителя Института, но А. Шварцу вменяли деяния, за которые он мог быть осужден на 50 лет лишения свободы¹⁷. То есть, несмотря на отсутствие прямого финансового вреда и отказ потерпевшего от обвинений, преступление было расценено как особо тяжкое, так как предметом стала уникальная информация значительных объемов.

Другим известным делом было использование уязвимости веб-сайта компании AT&T для сбора обще-

доступных данных (в том числе адресов электронной почты)¹⁸. А. Аннехаймер был признан судом штата виновным в совершении федерального преступления по Закону по борьбе с компьютерным мошенничеством и злоупотреблениями¹⁹. Позже приговор был отменен, но по причинам отсутствия юрисдикции у суда, рассматривавшего дело²⁰.

Обобщая законодательный и правоприменительный опыт США в области неправомерного доступа к компьютерной информации, очевидно, что информация как предмет преступления существенно влияет на квалификацию, подсудность и наказание. В зависимости от этого преступление может быть оценено как федеральное или подсудное штату. Характеристики информации влияют на размер наказания даже в отсутствие прямого экономически исчисляемого ущерба. Любая информация, независимо от характеристик ее обладателя и существования специального нормативного акта, подлежит правовой охране, если такой режим установил ее владелец.

В России зачастую применяется другой подход: в ст. 9 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» есть прямое указание, что «ограничение доступа к информации устанавливается федеральными законами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства». Подобная позиция подтверждена в Методических рекомендациях Генеральной прокуратуры РФ, где под охраняемой законом информацией понимается та, «для которой законом установлен специальный режим ее правовой защиты (например, государственная, служебная и коммерческая тайна, персональные данные и т. д.)»²¹. В данном документе информация подразделена на ту, для которой явно установлен режим правовой защиты, и остальную, которая не является предметом уголовно-правовой охраны.

Подобную точку зрения можно встретить и в некоторых судебных решениях. Так, в приговоре Верховного суда Чувашской Республики подчеркивается, что указание на охраняемость компьютерной информации должно быть явным, т. е. специальный режим

¹⁸ Позицию обвинения см.: URL: <https://www.eff.org/ru/document/auernheimer-superseding-indictment>.

¹⁹ URL: <https://www.theguardian.com/technology/2013/mar/18/us-hacker-andrew-auernheimer-at-t>.

²⁰ URL: <http://pdfserver.amlaw.com/nlj/auernheimer-op-usca3.pdf>.

²¹ Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации, утв. Генпрокуратурой России. URL: <http://genproc.gov.ru/documents/nauka/execution/document-104550/>.

¹⁶ USA v. Swartz, 1:11-cr-10260, No. 53 (D.Mass. Sep. 12, 2012).

¹⁷ URL: <https://www.wired.com/2015/10/cfaa-computer-fraud-abuse-act-most-controversial-computer-hacking-cases/>.

правовой защиты должен быть установлен законодательно. Согласно тексту приговора предметом преступления, предусмотренного ст. 272 УК РФ, является только охраняемая законом компьютерная информация²².

В правоприменительной практике существуют примеры, когда суд прямо требовал от обвинения сослаться на нормативные акты, закрепляющие охрану информации, к которой осуществлен неправомерный доступ. Например, по инициативе суда уголовное дело возвращено прокурору в связи с тем, что в предъявленном по ч. 2 ст. 272 УК РФ обвинении нет указания на положение закона или другого нормативного правового акта, в силу которого компьютерная информация, доступ к которой был предположительно осуществлен обвиняемым, является охраняемой законом информацией²³.

Спорна позиция, отраженная в российской практике применения уголовного закона, что уголовно-правовой охране подлежит только информация, защита которой прямо указана в федеральных законах и иных нормативных актах. В условиях перехода России к цифровой экономике при квалификации прежде всего должны оцениваться свойства и характери-

стики информации, к которой осуществляется неправомерный доступ и которая уничтожена, блокирована, модифицирована либо скопирована. Владелец информации должен сам устанавливать круг лиц и режим доступа для нее.

В настоящее время в российском уголовном праве на квалификацию неправомерного доступа к охраняемой законом информации в первую очередь влияют последствия деяния или характеристики субъекта. Такой подход соответствует традиционной парадигме, где информация лишь средство осуществления общественных отношений или государственного управления.

В концепции «цифровой экономики» информация — это основная ценность и продукт производства²⁴. Следовательно, ключевым фактором, учитываемым при квалификации и назначении наказания, должна являться информация, к которой осуществляется доступ. Такой подход демонстрирует законодатель США. В «цифровом» обществе свойства информации отражают общественную опасность преступлений в сфере компьютерной информации. По мере того как в России будет внедряться цифровая экономика, т. е. развиваться общественные отношения, связанные с оборотом и производством информации, возрастет роль информации как предмета преступления, предусмотренного ст. 272 УК РФ.

²² См. апелляционный приговор Верховного суда Чувашской Республики от 3 июня 2015 г. по делу № 22-1054/2015.

²³ См. апелляционное постановление Судебной коллегии по уголовным делам Верховного суда Республики Тыва от 26 октября 2017 г. по делу № 22-1534/2017.

²⁴ См., например: Linkov I., Trump B. D., Poinssatte-Jones K. Op. cit.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

- Ali M. A., Hoque M. R., Alam K. An Empirical Investigation of the Relationship Between E-Government Development and the Digital Economy: the Case of Asian Countries // *Journal of Knowledge Management*, 2018. Vol. 22. Iss. 5. URL: <https://www.emeraldinsight.com/doi/abs/10.1108/JKM-10-2017-0477>.
- Comprehensive Study on Cybercrime. URL: http://www.unodc.org/documents/organized-crime/cybercrime/CYBERCRIME_STUDY_210213.pdf.
- Digital Economy. URL: <https://www.commerce.gov/tags/digital-economy>.
- Kerr O. S. Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes // *New York University Law Review*. 2003. Vol. 78.
- Linkov I., Trump B. D., Poinssatte-Jones K. Governance Strategies for a Sustainable Digital World // *Sustainability* (Switzerland). 2018. Vol. 10. Iss. 2. URL: <http://www.mdpi.com/2071-1050/10/2/440/html>.
- Брославский Л. И. Уголовная ответственность за экологические преступления в области охраны вод в США // *Журнал российского права*. 2008. № 3.
- Владимир Путин. Внедрить цифровые технологии во все сферы жизни. URL: <https://rg.ru/2017/06/04/reg-szfo/vladimir-putin-vnedrit-cifrovye-tehnologii-vo-vse-sfery-zhizni.html>.
- Дремлюга Р. И. Понятие «компьютерная информация»: спорные вопросы в теории и законе // *Библиотека уголовного права и криминологии*. 2018. № 1.