Вестник Восточно-Сибирского института МВД России. 2024. № 2 (109). С. 109–119.
Vestnik of the East Siberian Institute of the Ministry of Internal Affairs of Russia. 2024. No. 2 (109). P. 109–119.

5.1.4. Уголовно-правовые науки

Научная статья
УДК 343.3/.7
DOI: 10.55001/2312-3184.2024.84.44.010

СРАВНИТЕЛЬНО-ПРАВОВОЙ АНАЛИЗ НОРМ ОБ УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ ЗА ПРЕСТУПЛЕНИЯ В СФЕРЕ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОНЫХ ТЕХНОЛОГИЙ

Вакутин Артем Андреевич[1], Бархатова Екатерина Николаевна[2]
[1]Омская академия МВД России, Омск, Российская Федерация
[2]Восточно-Сибирский институт МВД России, Иркутск, Российская Федерация
[1]artv@bk.ru
[2]solncevelvet@rambler.ru

Введение. С учетом стремительного развития информационно-телекоммуникационных технологий возникает необходимость защиты прав и свобод граждан в киберпространстве. Существующие на сегодняшний день российские уголовно-правовые нормы нуждаются в совершенствовании, предложения по которому могут быть сформулированы в результате их сравнительно-правового анализа с аналогичными нормами зарубежного законодательства.

Материалы и методы. В ходе исследования использовались работы отечественных ученых, материалы судебно-следственной практики, данные уголовной статистики, нормативные документы России и зарубежных государств. При написании статьи использовались общенаучные методы: системный подход, индукция, аналогия, анализ, синтез.

Результаты исследования. Проведен сравнительно-правовой анализ норм Уголовного кодекса Российской Федерации о различных преступлениях в сфере информационно-телекоммуникационных технологий и Закона Соединенных штатов Америки об информационной безопасности компьютеров.

Выводы и заключения. Сделан вывод о том, что формулировки, используемые в отечественном законодательстве, отличаются четкостью и ясностью понятий, в то время как нормы зарубежного законодательства предполагают возможность неоднозначного толкования. Вместе с тем указано на возможность имплементации в российское законодательство положения об ответственности за торговлю информацией, которое в настоящее время в подобном виде отсутствует в уголовном законе.

Ключевые слова: компьютерная информация, информационно-телекоммуникационные технологии, персональные данные, торговля цифровой информацией, компьютерная безопасность, киберпреступность.

Для цитирования: Вакутин А. А., Бархатова Е. Н. Сравнительно-правовой анализ норм об уголовной ответственности за преступления в сфере информационно-телекоммуникационных технологий // Вестник Восточно-Сибирского института МВД России: науч.-практич. журн. Иркутск: Восточно-Сибирский институт МВД России. 2024. № 2 (109). С. 109–119.
DOI: 10.55001/2312-3184.2024.84.44.010

5.1.4. Criminal law sciences

Original article

COMPARATIVE LEGAL ANALYSIS OF THE STANDARDS ON CRIMINAL LIABILITY FOR CRIMES IN THE FIELD OF INFORMATION AND TELECOMMUNICATION TECHNOLOGY

Artem A. Vakutin[1], Ekaterina N. Barkhatova[2]
[1]Omsk Academy of the Ministry of Internal Affairs of Russia, Omsk, Russian Federation
[2]East Siberian Institute of the Ministry of Internal Affairs of Russia, Irkutsk, Russian Federation
[1]artv@bk.ru
[2]solncevelvet@rambler.ru

Introduction: Given the rapid development of information and telecommunication technologies, there is a need to protect the rights and freedoms of citizens in cyberspace. The current Russian criminal law norms need improvement, proposals for which can be formulated as a result of their comparative legal analysis with similar norms of foreign legislation.

Materials and Methods: In the course of the study the works of domestic scientists, materials of judicial and investigative practice, data of criminal statistics, normative documents of Russia and foreign countries were used. When writing the article the following general scientific methods were used: systematic approach, induction, analogy, analysis, synthesis.

The Results of the Study: A comparative legal analysis of the provisions of the Criminal Code of the Russian Federation on various crimes in the field of information and telecommunication technologies and the Law of the United States of America on computer information security was carried out.

Findings and Conclusions: It is concluded that the wording used in domestic legislation is distinguished by clarity and clarity of concepts, while the norms of foreign legislation suggest the possibility of ambiguous interpretation. At the same time, the possibility of implementing into Russian legislation a provision on liability for trading in information, which is currently absent in the criminal law, is indicated.

Keywords: computer information, information and telecommunication technologies, personal data, trade in digital information, computer security, cybercrime.

For citation: Vakutin A. A., Barkhatova E. N. Sravnitel'no-pravovoj analiz norm ob ugolovnoj otvetstvennosti za prestuplenija v sfere informacionno-telekommunikacionnyh tehnologij [Comparative legal analysis of the norms on criminal liability for crimes in the field of information and telecommunication technologies]. Vestnik Vostochno-Sibirskogo instituta MVD Rossii - Vestnik of the East Siberian Institute of the Ministry of Internal Affairs of Russia. 2024, no. 2 (109), pp. 109–119.
DOI: 10.55001/2312-3184.2024.84.44.010

В условиях стремительного технологического развития и перехода к цифровой экосистеме вопросы информационной безопасности и защиты от неправомерного доступа к компьютерной информации становятся ключевыми в правовом пространстве.

Криминологический анализ данного вида преступности в России позволяет констатировать, что в последнее время для нее характерно свойство нелинейного роста [1, с. 41].

По оценкам специалистов, в настоящее время четко прослеживается тенденция увеличения количества преступлений, совершаемых с использованием информационно-телекоммуникационных технологий и в ближайшей перспективе изменения данной тенденции не предвидится [2, с. 60].

Так, в 2023 г. зарегистрировано 676 951 преступление, совершенное с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, что на 29,7 % больше, чем в 2022 г. Среди указанных преступлений 50, 6 % относятся к категории тяжких и особо тяжких.

Структура преступлений, совершенных использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации в 2023 г. в России, выглядит следующим образом.

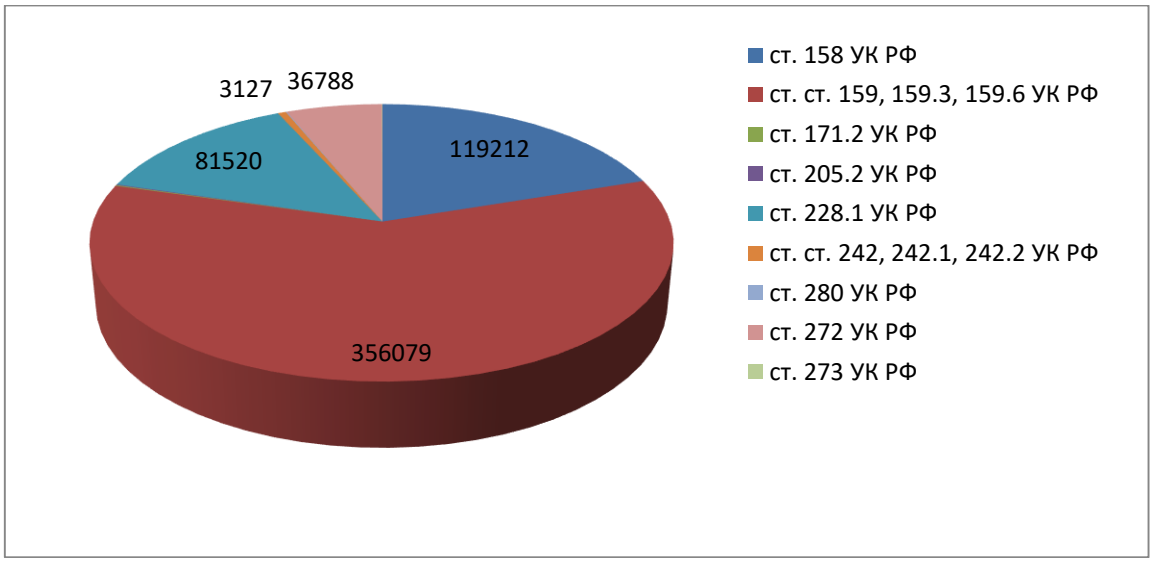

Рис. 1. Структура преступлений, совершенных использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации в 2023 г. в России

Особую тревогу вызывает стремительный рост числа фактов неправомерного доступа к компьютерной информации (ст. 272 УК РФ). По сравнению с 2022 г. количество таких преступлений выросло на 295,2 %. Нераскрытыми остаются 476 378 преступлений (+ 28,7 % по сравнению с аналогичным показателем 2022 г.)[1].

[1] Статистические данные МВД России // Министерство внутренних дел Российской Федерации : сайт. URL: https://мвд.рф/reports/item/47055751/ (дата обращения: 09.02.2024).

По некоторым подсчетам общий ущерб от киберпреступности в мировом масштабе составляет около 388 млрд долларов в год [3, с. 46].

В данном контексте в фокусе внимания оказываются уголовно-правовые нормы, регулирующие ответственность за подобные деяния. Для Российской Федерации – это Уголовный кодекс Российской Федерации (далее – УК РФ), и, в частности, глава 28 «Преступления в сфере компьютерной информации», а также ряд статей иных глав (например, 159^6 УК РФ «Мошенничество в сфере компьютерной информации»).

Несмотря на то, что законодательство Российской Федерации, направленное на противодействие преступлениям в сфере информационно-телекоммуникационных технологий, сформировано в достаточном объеме и позволяет правоприменителю эффективно работать в данном направлении, хотелось бы обратить внимание на перспективу дальнейшего его совершенствования с учетом наработок как отечественных, так и зарубежных ученых. Тем более что, по мнению отдельных авторов, действующее законодательство в области персональных данных не способно в полной мере защитить граждан от кражи паролей от банковских карт и аккаунтов в социальных сетях, фотографий и другой информации [4, с. 233].

Не затрагивая контекст существующих проблем международно-правовых отношений, обратимся к документу, который, по нашему мнению, содержит интересные с точки зрения предупреждения преступности, положения. Эти положения, в свою очередь, могут быть взяты на вооружение российским законодателем. Речь идет о Законе Соединенных штатов Америки об информационной безопасности компьютеров.

Стоит сделать отступление, что в Соединенных Штатах, в отличие от многих других стран, в том числе и России, отсутствует единый уголовный кодекс, который объединял бы в себе все уголовно-правовые нормы. Уголовное законодательство в США представлено разнообразием законов, принимаемых на федеральном уровне и на уровне штатов. С одной стороны, такая структура позволяет штатам иметь собственные уголовные кодексы, соответствующие особенностям и потребностям конкретного региона, с другой – предельно усложняет правоприменение, а нередко и вводит в заблуждение жителей одного региона при переезде в другой.

Закон США об информационной безопасности компьютеров (Computer Fraud and Abuse Act, далее – CFAA[1]) является одним из старейших нормативных актов в данной сфере, причем сохранившим изначальные нормы и смысл, в связи с чем интересно его сравнение с аналогичным российским законодательством, с целью выявить общности и различия, а также тенденции развития данной области законодательства.

CFAA представляет собой ключевой инструмент в уголовном законодательстве США, отдельный закон, направленный на регулирование и пресечение неправомерного доступа к компьютерной информации. Принятый еще в 1986 г., в эпоху, когда информационные технологии только начали проникать в повседневную жизнь, CFAA стал своего рода пионером в области уголовной ответственности за незаконный доступ к компьютерной информации. Он был принят с учетом

[1] 100 Stat. 1213 – Computer Fraud and Abuse Act of 1986 // GovInfo : U.S. Government Pablishing Office/ URL: https://www.govinfo.gov/app/details/STATUTE-100/STATUTE-100-Pg1213 (дата обращения: 08.02.2024).

необходимости защиты компьютерных систем, данных и сетей от мошенничества, несанкционированного доступа и других форм киберпреступлений. Опасения о неприкосновенности частной жизни в условиях автоматизации работы с данными впервые были высказаны в монографии профессора Колумбийского университета Алана Вестина «Неприкосновенность частной жизни и свобода» (1967 г.). Рассуждая о необходимости защиты персональных данных в условиях распространения средств слежения после войны, автор отметил проблему коммерческой передачи тайно собранных персональных данных [5, с. 1008].

С развитием компьютерных сетей закон подвергался ряду правок, отражающих технологические и социальные изменения, а также изменения в потребностях правопорядка в сфере кибербезопасности. Так, в 1994 г. Computer Fraud and Abuse Act Amendments расширил определение «защищенного компьютера» (очень отдаленно – аналог «критической информационной инфраструктуры» в нашем законодательстве) и были значительно ужесточены наказания за данные преступления. В 2001 г. USA PATRIOT Act (Закон о борьбе с терроризмом)[1] внес изменения в CFAA, включая расширение возможности судебного преследования за компьютерные преступления. В 2008 г. поправки еще более расширили определением «защищенного компьютера», о котором речь пойдет ниже, и внесли ряд изменений, касающихся мошенничества в сфере онлайн-аукционов[2].

Эти изменения представляют собой лишь некоторые этапы в эволюции CFAA, были и другие. Тем не менее вопросы, связанные с эффективностью и правомерностью некоторых положений закона, вызывают дискуссии в правоприменительном и научном сообществе, и обсуждения о его реформе продолжаются[3]. Так, в 2013 г. отклонен проект закона «Aaron's Law» (предложен после самоубийства Аарона Шварца, активиста и программиста, обвиненного в нарушении CFAA[4]). Этот проект предлагал изменения, направленные на уточнение и умеренное смягчение некоторых положений CFAA.

Однако особенность развития CFAA в том, что исходные нормы дошли до настоящего времени в практически неизменном виде, представляя, помимо юридической, еще и историческую ценность.

---

[1] USA PATRIOT Act // An official website of the United States Government URL: https://www.fincen.gov/resources/statutes-regulations/usa-patriot-act (дата обращения: 08.02.2024).

[2] Computer Fraud and Abuse Act (CFAA) // TechTarget URL: https://www.techtarget.com/searchsecurity/definition/Computer-Fraud-and-Abuse-Act-CFAA (дата обращения: 08.02.2024).

[3] The (still) unanswered questions around the CFAA and ‘good faith’ security research // SC Media URL: https://www.scmagazine.com/analysis/the-still-unanswered-questions-around-the-cfaa-and-good-faith-security-research (дата обращения: 08.02.2024); Data Scraping & the Courts: State of Play with the CFAA // Berkeley CLCT URL: https://cltc.berkeley.edu/2022/02/15/recap-data-scraping-the-courts-state-of-play-with-the-cfaa/ (дата обращения: 08.02.2024); Hacking the CFAA // Infosecurity Magazine URL: https://www.infosecurity-magazine.com/magazine-features/hacking-the-cfaa/ (дата обращения: 08.02.2024); Not A Crime: the CFAA and Respectability Politics // Tech Policy.PRESS URL: https://www.techpolicy.press/not-a-crime-the-cfaa-and-respectability-politics/ (дата обращения: 08.02.2024).

[4] Aaron's Law: What It Means, How It Works // Investopedia URL: https://www.investopedia.com/terms/a/aarons-law.asp (дата обращения: 08.02.2024).

Для дальнейшего понимания статьи следует отметить, что закон делится на разделы – «sections» (соответствует статьям или группам статей отечественных законов), обозначаемые строчными буквами латинского алфавита, заключенными в скобки (a), подразделы – «subsections», части, обозначаемые цифрами (5) и пункты – «paragraphs» (обозначает именно пункты, а не параграфы), обозначаемые заглавными буквами латинского алфавита (A).

Основными составом преступления, предусмотренного CFAA, является аналог отечественной ст. 272 УК РФ «Неправомерный доступ к компьютерной информации». С учетом особенностей конструирования уголовно-правовых норм США в разделе (a) указанного закона перечисляются различные действия, относящиеся к таковому преступлению: получение неправомерного доступа к информации, относящейся к интересам национальной безопасности, к финансовой информации финансового учреждения или эмитента карты, к информации, содержащейся в компьютерах федеральных органов исполнительной власти США; получение доступа к иным компьютерам в случае причинения ущерба лицу на сумму более 1000 долларов, получения доступа к медицинским данным. В целом статья содержит примерно тот же перечень деяний, что и ст. 272, и ч. 1 ст. 274[1] УК РФ. Однако стоит отметить один состав, включенный в раздел (a) – «торговля информацией, добытой неправомерным путем», аналог которого в Российской Федерации отсутствует. Так, в ч. 2 ст. 272 УК РФ присутствует указание на неправомерный доступ к компьютерной информации, совершенный из корыстной заинтересованности, который, в частности, вменяют в случаях, когда информация, добытая преступным путем, была продана третьим лицам, вместе с тем прямого указания на торговлю информацией нет. Например, П. с целью последующей продажи информации о логине и пароле доступа к Интернет-сайту, при помощи компьютерной техники, путем подбора логина и пароля, совершил неправомерный доступ к охраняемой законом компьютерной информации, содержащейся в административной панели Интернет-сайта serdolik-club.ru, после чего изменил логин и пароль в административной панели указанного Интернет-сайта, что повлекло модификацию и блокировку компьютерной информации, содержащейся на данном Интернет-сайте, принадлежащем потерпевшему. Продать информацию П. не успел, так как был задержан. Органами предварительного следствия П. вменена ч. 2 ст. 272 УК РФ, но с учетом обстоятельств вынесено ходатайство перед судом об освобождении П. от уголовной ответственности с назначением судебного штрафа, которое судом удовлетворено[1].

В другом случае преступнику удалось продать сведения, полученные в результате неправомерного доступа к компьютерной информации. Но поскольку данные сведения содержали коммерческую тайну, содеянное было квалифицировано по совокупности преступлений, предусмотренных ч. 3 ст. 272 УК РФ и ч. 3 ст. 183 УК РФ[2]. Представляется, что такой способ решения вопроса об ответственности за

[1] Постановление Устиновского районного суда г. Ижевска Удмуртской Республики от 17 ноября 2017 г. по делу № 1-256/17 // URL: https://sud-praktika.ru/precedent/546816.html (дата обращения: 09.02.2024).

[2] Приговор Орджоникидзевского районного суда г. Екатеринбурга от 25 июля 2017 г. по делу № 1-405/2017 // URL: https://sud-praktika.ru/precedent/366904.html (дата обращения: 09.02.2024).

торговлю информацией вполне эффективен, т. к. информация, составляющая различного рода тайну, охраняется уголовным законом. Вместе с тем не можем не согласиться, что указание на торговлю информацией в качестве квалифицирующего признака в ст. 272 УК РФ было бы уместным с точки зрения подчеркивания степени общественной опасности.

Справедливо утверждение А. А. Харламовой о том, что следственные и судебные органы не всегда уделяют достаточное внимание раскрытию содержания признака «из корыстной заинтересованности». В лучшем случае в описательной части решений судов корыстная заинтересованность находит отражение в виде следующих формулировок: «на условиях получения денежного вознаграждения», «выразившейся в желании получить доступ к ИТКС «Интернет» на более высокой скорости передачи данных» и т. п. [6, с. 165].

Подобная точка зрения поддерживается и М. М. Гедгафовым, указывающим, что чаще всего цифровая информация похищается с целью ее сбыта заказчикам, т. е. данный вид преступления стал отдельным видом «бизнеса» [7, с. 197].

Аналогом ст. 273 УК РФ «Создание, использование и распространение вредоносных компьютерных программ» выступает формулировка «передача программы, информации, кода или команды, если в результате такой деятельности причиняется ущерб защищенному компьютеру» ((a)(5)(A) CFAA. Норма дошла до настоящего времени в неизменном виде с 1986 г. и имеет чрезмерно размытые формулировки, что отмечают и исследователи в самом США.

Имеется также аналог ст. 159^6 УК РФ «Мошенничество в сфере компьютерной информации». CFAA содержит норму об ответственности за использование компьютера для мошенничества, включая создание ложных представлений и обман для получения доступа к защищенному компьютеру (a) (4).

Прямого указания на составы преступлений, совершаемых по неосторожности, в законе нет, тем не менее расплывчатые формулировки «умышленно получивший доступ к защищенному компьютеру без разрешения и в результате такой деятельности небрежно причинил ущерб» ((a)(5)(B)) этого закона предоставляют возможность привлечения за преступления, аналогичные ст. 274 УК РФ («Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей»).

Ключевым термином CFAA является «защищенный компьютер», который определен в разделе 18 U.S.C. §1030(e)(2) и охватывает два основных сценария использования. Подраздел (A) включает компьютер, предназначенный исключительно для использования финансовым учреждением или правительством Соединенных Штатов. В случае компьютера, неисключительно предназначенного для такого использования, он также рассматривается как защищенный, если используется финансовым учреждением или правительством Соединенных Штатов, и деятельность, составляющая преступление по CFAA, влияет на его использование финансовым учреждением или правительством. Посягательства на «защищенный компьютер» имеют согласно законодательству США значительно большую общественную опасность, и, соответственно, сроки наказания.

Подраздел (B) определения включает компьютер, который используется в межгосударственной или иностранной торговле или связи. Это означает, что даже если компьютер не связан с финансовым учреждением или правительством, он все равно считается защищенным, если его деятельность оказывает воздействие на межгосударственную или иностранную сферу обмена информацией и коммуникации. Таким образом, данное определение в CFAA учитывает не только функциональное предназначение компьютера, но и его влияние на международные и межгосударственные аспекты информационной области. Такие посягательства являются аналогом посягательств на критическую информационную инфраструктуру Российской Федерации (ст. 274[1] УК РФ), введенную в УК РФ Федеральным законом от 26 июля 2017 г. № 194-ФЗ[1].

CFAA предусматривает и квалифицирующие признаки, которые могут повлиять на характер и сроки наказания и учитывающие различные обстоятельства преступления, делая их более серьезными или устанавливая дополнительные аспекты, требующие особого внимания. Таковыми являются к примеру: «Если нарушение совершено с целью получения информации, относящейся к национальной обороне или иностранной торговле, или если нарушитель является иностранным агентом», «Если мошенничество совершается с использованием обманных представлений, создаваемых в ходе нарушения», «Если угрозы направлены на национальную безопасность, правительственные компьютерные системы или системы, обслуживающие здравоохранение, финансы или транспорт», «Если вредоносная программа приводит к значительному ущербу, включая серьезные нарушения функционирования компьютерных систем». Имеется и ряд квалифицирующих признаков, непосредственно определяющих зависимость срока наказания от ущерба.

С учетом внесенных изменений в CFAA представляется возможным выделить тенденции законодательства США об уголовной ответственности за преступления в сфере компьютерной информации:

1) постоянное расширение определения «защищенного компьютера». В различные моменты времени CFAA подвергался изменениям, расширяющим определение «защищенного компьютера». В данную дефиницию включены компьютеры, используемые финансовыми учреждениями, правительственными агентствами и другими организациями и т. д.;

2) ужесточение наказаний и введение новых отягчающих обстоятельств. На протяжении нескольких лет внесения изменений в CFAA сопровождались ужесточением наказаний для нарушителей. Это включало в себя увеличение штрафов и сроков тюремного заключения;

3) реакция на террористические угрозы и иные меры: в связи с угрозой терроризма были внесены изменения, направленные на расширение полномочий для борьбы с компьютерными преступлениями в целях национальной безопасности.

[1] О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» : Федеральный закон от 26 июля 2017 г. № 194-ФЗ // КонсультантПлюс: сайт. URL: https://www.consultant.ru/ document/cons_doc_LAW_220891/ (дата обращения: 12.03.2024).

Следует отметить, что тенденции в целом совпадают с таковыми в уголовном законодательстве Российской Федерации. С учетом все возрастающей общественной опасности подобных преступлений в нашей стране вводятся новые квалифицирующие признаки и нормы (например, ст. 274^1 УК РФ), появился новый отягчающий уголовную ответственность признак для обширного числа уголовных преступлений – с использованием средств массовой информации либо электронных или информационно-телекоммуникационных сетей. Внимание правоприменителя в нашей стране подтверждается и дачей разъяснений в постановлении Пленума Верховного Суда Российской Федерации спорных вопросов квалификации преступлений [1]. В научной среде активно указывается на необходимость изменения российского законодательства в части значительного усиления ответственности за нарушение законодательства о персональных данных, сбалансированность юридических и технических требований [8, с. 40; 9, с. 143; 10, с. 117].

Однако следует отметить и отличия законодательства. Так, статьи УК РФ гораздо проще для понимания обычного человека и правоприменителя. Формулировки куда менее размыты, а основные оценочные понятия разъяснены в указанном выше постановлении, что отсутствует в законодательстве США, где, несмотря на важность прецедентов, последние являются лишь отдельными судебными решениями с весьма низкой систематизацией. При этом разграничение различных деяний, наслаивавшихся с течением времени на рассматриваемый закон затруднительно, а правоприменение весьма субъективно.

В целом законодательство Российской Федерации в сфере уголовной ответственности за подобные виды преступлений с уверенностью можно назвать куда более проработанным, а проблемы правоприменения скрываются, скорее, не в уголовно-правовых актах, а в сфере деятельности уголовного процесса и технических возможностей доказывания, которых у США существенно больше в силу возможности доступа к большему числу систем обработки и хранения информации как на своей территории, так и на территориях других стран.

Тем не менее в рамках уголовно-правовых норм для имплементации в Российское законодательство представляет интерес ответственность за торговлю информацией, полученной путем неправомерного доступа к охраняемой законом компьютерной информации, что подтверждается наличием законопроекта об уголовной ответственности за подобные деяния[2]. Авторы законопроекта предлагают дополнить уголовный кодекс статьей 272^1 («Незаконные действия с компьютерной информацией, содержащей персональные данные»), что мы всецело поддерживаем.

---

[1] О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных электронных или информационно-телекоммуникационных сетей, включая сеть Интернет : Постановление Пленума Верховного Суда Российской Федерации от 15 декабря 2022 г. № 37 // URL: https://vsrf.ru/documents/own/31913/?ysclid=lse6tn9hdz899258912 (дата обращения: 09.02.2024).

[2] О внесении изменений в Уголовный кодекс Российской Федерации : законопроект № 502113-8 // Система обеспечения законодательной деятельности Российской Федерации. URL: https://sozd.duma.gov.ru/bill/502113-8#bh_note (дата обращения: 08.02.2024).

СПИСОК ИСТОЧНИКОВ

1. Колчевский, И. Б., Бицадзе, Г. Э. Преступления в сфере информационных технологий: понятие, структура // Научный портал МВД России. 2021. № 2. С. 40–47.

2. Урбан, В. В. Преступления, совершаемые с использованием информационно-телекоммуникационных сетей: общая характеристика и уголовно-процессуальные меры по их противодействию // Вестник Восточно-Сибирского института МВД России : науч.-практ. журн. 2019. № 1. С. 55–63.

3. Нуянзин, С. В., Виноградов, А. О., Тришкин, С. В. Преступность в сфере информационно-телекоммуникационных технологий: современное состояние и некоторые меры по противодействию ей // Научный портал МВД России. 2020. № 2. С. 45–54.

4. Богданов, А. В., Виноградов, Е. А., Хазов, Е. Н. Телекоммуникационные технологии и компьютерная грамотность как средство профилактики киберпреступлений // Образование и право. 2021. № 8. С. 231–236.

5. Магомедова, О. С., Коваль, А. А., Левашенко, А. Д. Торговля данными: разные подходы, одна реальность // Вестник Российского университета дружбы народов. Серия: Юридические науки. 2020. Т. 24. № 4. С. 1005–1023.

6. Харламова, А. А. Неправомерный доступ к компьютерной информации: толкование признаков и некоторые проблемы квалификации // Вестник Уральского юридического института МВД России. 2020. № 2. С. 162–166.

7. Гедгафов, М. М. Особенности выявления и раскрытия преступлений, связанных с приобретением или сбытом цифровой информации, заведомо добытой незаконным путем // Пробелы в российском законодательстве. 2020. Т. 13. № 5. С. 196–199.

8. Солдатова, В. И. Защита персональных данных в условиях применения цифровых технологий // Lex Russica. 2020. № 2. С. 33–43.

9. Терещенко, Л. К. Государственный контроль в сфере защиты персональных данных // Право. Журнал Высшей школы экономики. 2018. № 4. С. 142–161.

10. Талапина, Э. В. Защита персональных данных в цифровую эпоху: российское право в европейском контексте // Труды института государства и права Российской академии наук. 2018. Т. 13. № 5. С. 117–143.

REFERENSES

1. Kolchevskij, I.B, Bicadze, G.Je. Prestuplenija v sfere informacionnyh tehnologij: ponjatie, struktura [Crimes in the field of information technology: concept, structure]. Nauchnyj portal MVD Rossii - Scientific portal of the Ministry of Internal Affairs of Russia. 2021, no. 2, pp. 40-47. (in Russian).

2. Urban V.V. Prestuplenija, sovershaemye s ispol'zovaniem informacionno-telekommunikacionnyh setej: obshhaja harakteristika i ugolovno-processual'nye mery po ih protivodejstviju [Crimes committed using information and telecommunication networks: general characteristics and criminal procedural measures to counter them]. Vestnik Vostochno-Sibirskogo instituta MVD Rossii - Vestnik of the East Siberian Institute of the Ministry of Internal Affairs of Russia. 2019, no. 1, pp. 55-63. (in Russian).

3. Nujanzin, S.V., Vinogradov, A.O., Trishkin, S.V. Prestupnost' v sfere informacionno-telekommunikacionnyh tehnologij: sovremennoe sostojanie i nekotorye mery po protivodejstviju ej [Crime in the field of information and telecommunication technologies: current state and some measures to counter it]. Nauchnyj portal MVD Rossii - Scientific portal of the Ministry of Internal Affairs of Russia. 2020, no. 2, pp. 45-54. (in Russian).

4. Bogdanov, A.V., Vinogradov, E.A., Hazov, E.N. Telekommunikacionnye tehnologii i komp'juternaja gramotnost' kak sredstvo profilaktiki kiberprestuplenij [Telecommunication technologies and computer literacy as a means of preventing cybercrimes]. Obrazovanie i pravo - Education and Law. 2021, no. 8, pp. 231-236. (in Russian).

5. Magomedova, O.S., Koval', A.A., Levashenko, A.D. Torgovlja dannymi: raznye podhody, odna real'nost' [Data trading: different approaches, one reality]. Vestnik Rossijskogo universiteta

druzhby narodov. Serija: Juridicheskie nauki. - Vestnik of the Peoples' Friendship University of Russia. Series: Legal sciences. 2020, vol. 24, no. 4, pp. 1005-1023. (in Russian).

6. Harlamova, A.A. Nepravomernyj dostup k komp'juternoj informacii: tolkovanie priznakov i nekotorye problemy kvalifikacii [Illegal access to computer information: interpretation of signs and some qualification problems]. Vestnik Ural'skogo juridicheskogo instituta MVD Rossii. - Vestnik of the Ural Law Institute of the Ministry of Internal Affairs of Russia. 2020, no. 2, pp. 162-166. (in Russian).

7. Gedgafov, M.M. Osobennosti vyjavlenija i raskrytija prestuplenij, svjazannyh s priobreteniem ili sbytom cifrovoj informacii, zavedomo dobytoj nezakonnym putem [Features of identifying and solving crimes related to the acquisition or sale of digital information known to be obtained illegally]. Probely v rossijskom zakonodatel'stve - Gaps in Russian legislation. 2020, vol. 13, no. 5, pp. 196-199. (in Russian).

8. Soldatova, V.I. Zashhita personal'nyh dannyh v uslovijah primenenija cifrovyh tehnologij [Protection of personal data in the context of the use of digital technologies]. Lex Russica. - Lex Russica. 2020, no. 2, pp. 33-43. (in Russian).

9. Tereshhenko, L.K. Gosudarstvennyj kontrol' v sfere zashhity personal'nyh dannyh [State control in the field of personal data protection]. Pravo. Zhurnal Vysshej shkoly jekonomiki. - Right. Journal of the Higher School of Economics. 2018, no. 4, pp. 142-161. (in Russian).

10. Talapina, Je.V. Zashhita personal'nyh dannyh v cifrovuju jepohu: rossijskoe pravo v evropejskom kontekste [Protection of personal data in the digital age: Russian law in the European context]. Trudy instituta gosudarstva i prava Rossijskoj akademii nauk. - Proceedings of the Institute of State and Law of the Russian Academy of Sciences. 2018, vol. 13, no. 5, pp. 117-143. (in Russian).

ИНФОРМАЦИЯ ОБ АВТОРАХ

Вакутин Артем Андреевич, кандидат юридических наук, доцент, доцент кафедры уголовного права. Омская академия МВД России. 664074, Омск, пр-т Комарова, 7.

Бархатова Екатерина Николаевна, кандидат юридических наук, доцент, доцент кафедры уголовного права и криминологии. Восточно-Сибирский институт МВД России. 664074, Иркутск, ул. Лермонтова, 110.

INFORMATION ABOUT THE AUTHOR

Vakutin Artem Andreevich, Candidate of Law, Docent, Assistant Professor of Department of Criminal Law of the Omsk academy of the Ministry of Internal Affairs of Russia. 644092. Omsk, Komarov avenue, 7.

Barkhatova Ekaterina Nikolaevna, Candidate of Law, Docent, Assistant Professor of Department of Criminal Law and Criminology of the East-Siberian Institute of the Ministry of Internal Affairs of Russia. 664074, Irkutsk, Lermontov str., 110.

Статья поступила в редакцию 12.02.2024; одобрена после рецензирования 19.03.2024; принята к публикации 24.05.2024.

The article was submitted 12.02.2024; approved after reviewing 19.03.2024; accepted for publication 24.05.2024.