КОМПАРАТИВИСТСКИЕ ИССЛЕДОВАНИЯ УГОЛОВНОГО ПРАВА, КРИМИНОЛОГИИ И УГОЛОВНО-ИСПОЛНИТЕЛЬНОГО ПРАВА

ПРОТИВОДЕЙСТВИЕ КИБЕРПРЕСТУПНОСТИ ЗА РУБЕЖОМ

СЕМЫКИНА Ольга Ивановна, старший научный сотрудник отдела зарубежного конституционного, административного, уголовного законодательства и международного права Института законодательства и сравнительного правоведения при Правительстве Российской Федерации, кандидат юридических наук
117218, Россия, г. Москва, ул. Большая Черемушkinsкая, 34
E-mail: semykola@yandex.ru

Современные тенденции противодействия киберпреступности в уголовном законодательстве России и зарубежных государств настолько многоплановы, что порой весьма сложно провести разграничение между деяниями, непосредственно посягающими на информационную безопасность, и посягательствами, связанными с компьютерными технологиями, в которых использование компьютерных информационных систем является лишь одним из способов совершения преступления. Эта посылка подкрепляется аналитическим материалом, основанным на исследовании уголовно-правовых норм, так или иначе сконструированных в законодательстве Великобритании, Австралии, США, Германии и государств — участников СНГ с учетом признака незаконного доступа к информационным технологиям и (или) неправомерного использования информационно-телекоммуникационных сетей. Проведенный в настоящей статье комплексный компаративистский анализ различных уголовно-правовых норм, как сконцентрированных в одной группе с учетом тождества объекта посягательства, так и «растворенных» в структуре иных уголовно-правовых предписаний, исходя из способа совершения деяния, позволил выявить реальную картину тенденций противодействия преступлениям, совершаемым с использованием кибертехнологий (против конституционных прав и свобод личности, собственности, в сфере экономической деятельности, против здоровья населения и общественной нравственности, конституционного строя и безопасности государства).

Ключевые слова: противодействие, киберпреступность, компьютерные преступления, хищение, кража, мошенничество, присвоение, растрата, компьютерная информация, информационные технологии, информационно-телекоммуникационная сеть, несанкционированный доступ, модификация информации, блокирование информации.

COMBATING CYBERCRIME IN FOREIGN COUNTRIES

O. I. SEMYKINA, senior research fellow of the Institute of Legislation and Comparative Law under the Government of the Russian Federation, candidate of legal sciences
34, Bolshaya Cheremushkinskaya st., Moscow, Russia, 117218
E-mail: semykola@yandex.ru

Modern trends in Cybercrime in the criminal legislation of Russia and foreign countries are so multifaceted that sometimes it is difficult to distinguish between acts that directly violate information security, and invasions associated with computer technology in which the use of computer information systems is only one of the ways committing a crime. It is supported by the analytical material based on the study of criminal law engineered in the legislation of the UK, Australia, the USA, Germany and the CIS countries in view of the characteristic of illegal access to information technologies and (or) the misuse of information and telecommunication networks. Carried out in this article a comparative analyzes of the different criminal law as concentrated in one group, taking into account the identity of the object of the offence and “dissolved” in the structure of other criminal law provisions reveal the real “picture” of trends in the sphere of combating Cybercrime (against the constitutional rights and freedoms, property, area of economic activity, against public health and public morality, constitutional order and security of the state).

Keywords: combating, Cybercrime, computer crime, theft, fraud, misappropriation, embezzlement, computer information, information technology, information and telecommunications network, unauthorized access, modification information, block information.

DOI: 10.12737/23525

С учетом современных процессов информатизации общества сфера компьютерных технологий используется как плацдарм для совершения многих преступлений, входящих в структуру киберпреступности. С одной стороны, речь

идет о тех киберпреступлениях, которые непосредственно посягают на информационную безопасность личности, общества и государства (к этой категории относятся, например, несанкционированный доступ к компьютерной информации, не-

законный оборот технических средств, модификация компьютерной информации, компьютерный саботаж и др.). С другой стороны, можно говорить о преступлениях, связанных с кибертехнологиями. Использование при их совершении информационно-телекоммуникационных систем характеризует киберпреступную направленность деяния (в частности, в данную группу входят кража, мошенничество, присвоение или растрата, совершенные с использованием компьютерных технологий, незаконный оборот компьютерных программ, предназначенных для осуществления транзакций, манипулирование рынком, хищение радиоактивных материалов, наркотических средств, психотропных веществ, их аналогов и прекурсоров, незаконный интернет-оборот порнографических материалов, незаконное получение государственных, коммерческих и банковских секретов посредством применения информационных технологий и проч.)¹. В каждом государстве наблюдаются различные подходы к криминализации этих деяний, посягающих на разные сферы общественных отношений (собственность, экономику, здоровье населения, общественную нравственность, информационную безопасность), что не просто выявляет структурные особенности киберпреступности в той или иной стране, а прежде всего актуализирует национальные уголовно-правовые меры противодействия образующим ее киберпреступлениям, совершаемым в отношении компьютерной системы и (или) с намерением завладеть компьютерными данными². В этой области несомненный интерес вызывает компаративистский анализ основных тенденций в установлении уголовной ответственности за хищения (кражи, мошенничество, присвоения или растраты) и иные противоправные деяния, совершенные с использованием кибертехнологий, в законодательстве России и некоторых зарубежных государств.

Итак, в уголовном законодательстве зарубежных государств «площадка» криминализации не только включает деяния, непосредственно посягающие на информационную безопасность (консолидированные с учетом тождества родового объекта посягательства), но и охватывает иные общественно опасные посягательства, сопряженные с использованием информационно-телекоммуникационных сетей (в которых информационная сфера является факультативным объектом преступления). В настоящее

время вектор «растворения» таких норм в структуре уголовных законов зарубежных стран направлен на: 1) введение ответственности за хищение в сфере компьютерных технологий в специальной уголовно-правовой норме; 2) установление признака использования информационных технологий в качестве криминообразующего признака хищения; 3) признание компьютерной информации предметом преступного посягательства либо криминализации использования компьютерных технологий одним из способов, средством³ или квалифицирующим признаком совершения различных видов преступлений; 4) новеллирование видов киберпреступлений.

Остановимся на каждой из приведенных тенденций более подробно.

1. В некоторых зарубежных странах ответственность за хищение, совершенное путем использования различных информационных технологий, концентрируется в специальных уголовно-правовых нормах об ответственности за хищения — мошенничество (Россия, Молдавия) или так называемые преступления обманного характера (Великобритания, Австралия, США).

Так, в уголовном законодательстве государств — участников СНГ ответственность за хищение в сфере компьютерных технологий исчерпывается только одной его формой — мошенничеством. Этот путь характерен, например, для уголовного законодательства России и Молдавии. Как известно, Федеральным законом от 29 ноября 2012 г. № 207-ФЗ гл. 21 УК Российской Федерации помимо ст. 159⁴—159⁵, вызвавших бурную дискуссию в научных кругах⁴, была дополнена ст. 159⁶, предусматривающей ответственность за мошенничество в сфере компьютерной информации. Согласно этой статье уголовно наказуемым признается хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей. В отличие от УК РФ Уголовный кодекс Республики Молдова от 18 апреля 2002 г. № 985-XV рассматривает мошенничество с использованием информационных технологий не как преступление против собственности, а как информационное преступле-

¹ См.: Семькина О. И. Тенденции борьбы с преступлениями в сфере информационных технологий (сравнительно-правовой аспект) // Сборник трудов XXIII Всероссийской конференции «Информатизация и информационная безопасность правоохранительных органов». М., 2014. С. 49—54.

² См., например, ст. 1—10 Конвенции Совета Европы «О преступности в сфере компьютерной информации» 2001 г.

³ См., например: Хиллута В. В. Уголовная ответственность за хищения с использованием компьютерной техники // Журнал российского права. 2014. № 3. С. 111—118.

⁴ См., например: Сидоренко Э. Л. Мошенничество в сфере страхования: некоторые проблемы квалификации // Уголовное право. 2015. № 5. С. 90—94; Сидоренко Э. Л., Волеводз А. Г. Мошенничество в сфере предпринимательской деятельности: особенности судебного толкования // Мировой судья. 2016. № 2. С. 20—26.

ние и преступление в области электросвязи. В статье 260⁶ УК Молдовы под информационным мошенничеством понимаются противоправные умышленные действия, в результате которых был нанесен ущерб интеллектуальной собственности другого лица в крупных размерах посредством следующих средств и обстоятельств: 1) любого ввода, нарушения, отключения, удаления либо сокрытия компьютерной информации; 2) любого подключения к функционирующей компьютерной информационной системе, совершенного с обманом умыслом или в целях получения незаконной экономической выгоды для себя либо для другого лица⁵.

Таким образом, УК Молдовы придает информационному мошенничеству иную окраску:

родовым объектом этого преступления выступают общественные отношения, обеспечивающие права и законные интересы граждан, общества и государства в сфере создания и обращения компьютерной информации⁶;

в непосредственный объект входят общественные отношения в сфере обеспечения безопасности информационной системы и информационной сети, электромагнитных носителей информации, других составляющих машин, инструментов, способствующих нормальному и правомерному функционированию информационных систем и информационных сетей;

факультативный объект может включать личные права граждан — абонентов информационной системы и информационной сети — на обеспечение хранения личных информационных данных, на конфиденциальность сообщений, содержащихся на различных машинных носителях⁷;

по конструкции объективной стороны информационное мошенничество является материальным составом, и для признания этого деяния окончательным необходимо установить не момент завладения виновным чужим имуществом для себя либо другого лица, а факт причинения этим деянием ущерба в крупном размере.

В отличие от имущественного мошенничества (ст. 190 УК Молдовы) предметом информационного мошенничества признается информация, полученная, обрабатываемая и хранящаяся⁸ в компьютерной

сети или информационной системе, на электромагнитных носителях, а также в базе данных других технических средств информационной системы или сети, которые могут на законном основании выдавать сведения об имеющихся информационных данных, находящихся в информационной сети, о передаче, отправлении информации к абонентам либо пользователям информационной системы или сети⁹. Обязательным криминообразующим признаком информационного мошенничества является наличие в деянии лица цели извлечения материальной выгоды для себя либо иного лица (денег, реальных предметов или иных ценностей). При этом неправомерные ввод, изменение или удаление информационных данных либо ограничение доступа к этим данным, совершенные не в целях извлечения материальной выгоды, а повлекшие выдачу недостоверных данных в целях их использования, например в дальнейшей преступной деятельности, квалифицируются иначе — как подлог информационных данных (ст. 260⁵ УК Молдовы).

В разработках молдавских ученых¹⁰ отмечается, что информационное мошенничество может совершаться пассивными способами — путем внедрения вредоносных программ (например, посредством размещения файлов вредоносной программы в локальных сетях ЭВМ, на электронных досках объявлений (BBS), в глобальных информационных сетях, на ЭВМ общего пользования на предприятиях, в учреждениях и организациях; посредством рекламы и распространения машинных носителей, содержащих вредоносные программы (пиратских дисков, контрафактного программного обеспечения); распространения вредоносных программ вместе с самой ЭВМ). Не менее популярным при совершении информационного мошенничества является использование активных способов, связанных с непосредственным воздействием субъекта на компьютерную технику (в частности, когда виновный самостоятельно осуществляет взаимодействие с ЭВМ, системой ЭВМ или их сетью, загружая вредоносную программу и используя ее, а потерпевший либо не знает о самом факте внедрения вредоносной программы, либо не осознает ее вредоносный характер)¹¹.

ступления, изложенному в п. «а» ст. 1 Соглашения о сотрудничестве государств — участников СНГ в борьбе с преступлениями в сфере компьютерной информации 2001 г. (г. Минск), предметом посягательства которого является компьютерная информация.

⁹ См.: Маймеску С. Указ. соч.

¹⁰ См., например: Дмитришен М., Гончаров И. Мошенничество в информационных технологиях. URL: <http://security.ase.md/>.

¹¹ Подробнее об активных и пассивных способах совершения мошенничества с использованием информационных технологий см.: Дмитришен М., Гончаров И. Указ. соч.

⁵ См.: Маймеску С. Глава XXI. Информационные преступления и преступления в области электросвязи // Комментарий к Уголовному кодексу Республики Молдова. Общая и Особенная части. Кишинэу, 2010. С. 792—794.

⁶ См.: Гришук-Бучка С. Уголовно-правовая характеристика преступлений против компьютерной безопасности (по законодательству Республики Молдова). URL: <http://security.ase.md/materials/si2010/material-2010.pdf>.

⁷ См.: Маймеску С. Указ. соч.

⁸ Следует отметить, что такой подход молдавского законодателя соответствует определению информационного пре-

В Великобритании ответственность за обманные деяния предусмотрена Законом о преступлениях обманного характера 2006 г. Названный Закон распространил норму об ответственности за владение, изготовление и поставку предметов, используемых в обманных преступлениях (ст. 6), на владение и осуществление контроля над любыми компьютерными программами и электронными данными¹². Причем исследователи английского уголовного права отмечают некоторые особенности квалификации обманных деяний в соответствии с этим Законом. Так, по мнению Э. Дж. Эшворта, структура преступлений обманного характера необычна тем, что позволяет считать деяние оконченным независимо от того, получена ли в результате деяния реальная выгода и причинены ли реальные убытки¹³.

Кроме того, нормы об ответственности за владение и поставку другим лицам предметов в целях обманного получения закрытой информации путем использования телекоммуникационных систем содержатся в Законе о телекоммуникациях (обманах) 1997 г., конкретизирующем, что использование предметов включает оборот предметов, применяемых для записи любых данных, а также последующее использование этих данных с намерением бесчестного получения услуг (ст. 1(6)). Также в части квалификации хищений с использованием компьютерных технологий применяются предписания Закона о краже 1968 г. и Закона о краже 1978 г. Речь идет о бесчестных имущественных преступлениях, при совершении которых используются компьютерные технологии (краже, получении имущества или услуг путем обмана, преступлениях, связанных с украденным имуществом, вымогательстве)¹⁴.

В федеральном законодательстве Австралии ответственность за мошеннические действия предусмотрена в ст. 133—134 Уголовного кодекса 1995 г. По мнению исследователей австралийского уголовного права, юридическая природа мошенничества в сфере компьютерной информации включает завладение с корыстной целью деньгами, товарами, услугами или другими выгодами посредством использования измененных, фиктивных или полученных неправомерным путем оригинальных сведений и машинных (пластиковых) носителей (например, ис-

пользование похищенных кредитных банковских карт или их номеров в целях получения финансовой выгоды). Такого рода деяния включаются в понятие электронных обманов и могут совершаться в следующих видах: 1) обманы с платежными банковскими системами путем использования фиктивных документов (выпуск машинных (пластиковых) носителей с превышением кредитного баланса на счете в целях приобретения товаров или услуг, скриминг с кредитными банковскими картами); 2) обманы с прямым дебетом (осуществление дебетовых онлайн-платежей); 3) обманы с электронными переводами (незаконное получение паролей, ложное отождествление идентификационных данных); 4) обманы, совершенные путем онлайн-маскировки (создание дублирующих веб-сайтов)¹⁵.

Следует отметить, что федеральное уголовное законодательство Австралии отличает бесчестную кражу от обманных преступлений, нацеленных на получение собственности или услуги (любых прав, льгот, привилегий) путем обмана. Кроме того, как рассматривалось выше, в федеральном австралийском законодательстве существуют специальные составы преступлений, охватывающие способы обмана с привлечением компьютерных технологий (например, обманы с кредитными картами), и отграничить в этой ситуации кражу от мошенничества бывает затруднительно¹⁶. По этому вопросу в ст. 134.1 (15) УК Австралии указывается, что, если при инкриминировании деяния орган уголовного преследования считает лицо виновным в краже, но вне всяких разумных сомнений обвиняемый совершил обманное деяние, за судом (судьей) закрепляется право признать лицо виновным в преступлении обманного характера при условии предоставления обвиняемому процессуальной справедливости в отношении этого факта установления вины. Аналогичное указание имеется применительно к вопросу переквалификации деяния обвиняемого с обманного преступления на кражу (ст. 134.1 (16) УК Австралии).

В федеральном законодательстве США компьютерные обманы включают бесчестное использование компьютерных технологий путем создания новых или искажения существующих данных с намерением получения чужого имущества. В Своде законов США (далее — U.S.C.) криминализированы следующие способы совершения компьютерных обманов: 1) намеренный несанкционированный доступ к компьютеру, превышение пределов авторизованного доступа или иные неправомерные манипуляции с компью-

¹² См.: Голованова Н. А. Особенная часть. Уголовное право Англии // Уголовное право зарубежных стран. Общая и Особенная части: учебник / под ред. И. Д. Козочкина. 3-е изд. М., 2010. С. 625.

¹³ См.: Ashworth A. J. United Kingdom // The Handbook of Comparative Criminal Law / eds. by K. J. Heller, M. D. Dubber. Stanford; California, 2011. P. 552.

¹⁴ См.: Власов И. С., Голованова Н. А., Меньших А. А. Ответственность за компьютерные преступления по законодательству зарубежных государств // Журнал зарубежного законодательства и сравнительного правоведения. 2005. № 2. С. 124.

¹⁵ См.: Mazzone A. Identity Fraud — Government Legislative Responses // Victorian Government Solicitor's Office. URL: <http://vgso.vic.gov.au/sites/default/files/publications/Identity%20Fraud%20-%20Government%20Legislative%20Responses.pdf>.

¹⁶ См.: Bronitt S., McSherry B. Principles of Criminal Law. 3rd ed. Sydney, 2006. P. 746—748.

терной информацией, которые могут использоваться в интересах иностранного государства, причинить либо создать угрозу причинения вреда национальной безопасности США (18 U.S.C. § 1030 (a) (1)); 2) намеренный несанкционированный доступ к компьютеру либо превышение пределов авторизованного доступа к финансовым отчетам финансовых учреждений, эмитентов карт, департаментов и агентств США, а равно к иным защищенным компьютерам (18 U.S.C. § 1030 (a) (2)); 3) умышленный несанкционированный доступ к государственной правительственной системе США (18 U.S.C. § 1030 (a) (3)); 4) сознательный с намерением обмана несанкционированный доступ к защищенному компьютеру в целях обманного получения какого-либо имущества, за исключением имущества стоимостью не более 5000 долл. США, полученного исключительно в результате использования компьютера в любой одногодичный период (18 U.S.C. § 1030 (a) (4)); 5) несанкционированное получение, передача программ, информации, компьютерных кодов, команд и иных сведений о доступе к защищенному компьютеру, причинившие повреждение такому компьютеру или ущерб (18 U.S.C. § 1030 (a) (5)); 6) сознательный с намерением обмануть несанкционированный трафик компьютерной информации, причинивший ущерб межгосударственной или внешней торговле (18 U.S.C. § 1030 (a) (6)); 7) передача электронных сообщений, содержащих угрозы повреждения защищенного компьютера, несанкционированного получения информации и нарушения конфиденциальности сведений, совершенная в целях вымогательства денежных средств или иного имущества, а равно содействия такому вымогательству (18 U.S.C. § 1030 (a) (7)); 8) перехват устных, телеграфных и электронных сообщений (18 U.S.C. § 2511 (1) (b) (iv)); 9) использование средств почтовой связи (18 U.S.C. § 1302); 10) неправомерные транзакции с кредитными картами в торговой сфере (15 U.S.C. § 1644).

В правоприменительной практике как компьютерные обманы квалифицируются следующие деяния: кража информации с компьютеров, принадлежащих финансовым учреждениям или федеральным агентствам, а также используемых в государственной торговой деятельности; кража средств электронного кошелька путем изменения учетных данных; несанкционированный доступ к информации, находящейся в государственных компьютерных системах; обманные почтовые лотереи (например, реализация схем так называемых финансовых пирамид путем рассылки электронных сообщений о том, как заработать деньги в кратчайшие сроки¹⁷); перехват информации об одобренном кредите; получение PIN-кодов кредитных карт путем подглядывания, отслеживания или использования подслушивающих устройств;

использование фальсифицированных средств телемаркетинга в целях получения частной информации о клиентской базе (фишинг); предложения фиктивных вакансий, направленные по электронной почте; сбор конфиденциальной информации и ее последующее использование для получения выгоды; трафик похищенных паролей; угрозы повреждения компьютеров в целях вымогательства¹⁸. Для совершения компьютерных обманов используются различные способы, например: несанкционированное изменение входа в компьютерную систему; модификация и удаление электронных сведений; несанкционированный перехват электронной передачи частной информации (паролей, данных кредитных карт и иных конфиденциальных сведений); умышленное или неосторожное повреждение электронных систем или баз данных; создание программных кодов и загрузка их в компьютерные системы банков в целях получения доступа к базам данных клиентов дистанционной системы обслуживания (информации по кредитным картам); компьютерные вирусы и черви¹⁹.

В Германии наряду с основным составом мошенничества (§ 263 УК) в преступлениях против имущества как целого сформулирован специальный состав — компьютерное мошенничество (§ 263a УК), введенное в уголовное законодательство в целях необходимости уголовного преследования за использование в мошеннических схемах компьютерных технологий и различных программных манипуляций²⁰. Согласно § 263a УК Германии под компьютерным мошенничеством понимается деяние, причиняющее имущественный ущерб путем формирования (установления) неправильных компьютерных программ, использования неверных или неполных данных, несанкционированного использования данных и иного неправомерного воздействия на процессы электронной обработки информации, совершенное в целях получения имущественной выгоды (как личной, так и в интересах третьих лиц)²¹. Как видно, мошеннические компьютерные манипуляции наделены специальными криминообразующими признаками. Во-первых, непосредственный результат воздействия на процесс

¹⁸ См.: Identity Theft (FAQ) // Nolo. Law for All. URL: <http://www.nolo.com/legal-encyclopedia/identity-theft-faq-29074.html>; What is Illegal under Local, State and Federal Laws? Federal Computer Security Violations // Cornell University. IT Cornell. URL: <http://www.it.cornell.edu/policies/university/privacy/responsible/illegal.cfm>.

¹⁹ См.: Computer and Internet Fraud // Cornell University Law School. Legal Information Institute. URL: http://www.law.cornell.edu/wex/computer_and_internet_fraud.

²⁰ См.: Odenthal R. Korruption und Mitarbeiterkriminalität: Wirtschaftskriminalität vorbeugen, erkennen und aufdecken. 2., vollständig überarbeitete und erweiterte Auflage. Gabler I GWV Fachverlage GmbH, Wiesbaden, 2009. S. 83, 275.

²¹ Ibid. S. 275.

¹⁷ См.: Federal Criminal Law and its Enforcement / N. Abrams, S. S. Beale, S. R. Klein. 5th ed. West, 2010. P. 23, 205.

обработки данных должен выражаться в нанесении ущерба чужому имуществу²². Во-вторых, в отличие от основного состава мошенничества, компьютерное мошенничество включает обман, направленный не на человека, а на программу, а ущерб в таком случае является результатом воздействия на процесс переработки информации. В иной ситуации — при направлении обмана на человека, а не на компьютерную систему или компьютерную информацию — содеянное квалифицируется как основное мошенничество²³ (§ 263 УК Германии).

Исследователи германского уголовного права выделяют следующие формы компьютерного мошенничества: 1) мошенничество с товарами, приобретенными на онлайн-аукционах или в интернет-магазинах; 2) мошенничество с кредитными картами²⁴, в том числе в банкоматах²⁵; 3) новые методы мошенничества со счетами и отмыванием денег, например создание компаний по депонированию денежных средств; 4) рекламное мошенничество путем наиболее типичных обманных схем с адресными книгами; 5) мошенничество в сфере добросовестной конкуренции, в частности, направленное на обманное предоставление конкурентного преимущества; 6) клик-мошенничество, когда используется интернет-реклама (или «спонсорские списки») услуг, к примеру, страхования в «один клик»²⁶.

2. Сегодня в уголовном законодательстве некоторых зарубежных государств наблюдается тенденция признания использования информационных технологий, компьютерной техники и информационных сетей, в том числе сетей Интернет, в качестве криминообразующих признаков различных форм и видов хищения, а также «фигурирования» информационных технологий в составах завладения чужим имуществом без цели хищения. К данной группе государств относятся такие государства — участники СНГ, как Белоруссия и Узбекистан.

Уголовный кодекс *Республики Беларусь* от 9 июля 1999 г. № 275-З, например, в примечании 1 к гл. 24 «Преступления против собственности» закрепляет родовую дефиницию хищения. Согласно этому указанию хищение как преступление против собственности — это умышленное противоправное безвоз-

мездное завладение чужим имуществом или правом на имущество с корыстной целью путем кражи, грабежа, разбоя, вымогательства, мошенничества, злоупотребления служебными полномочиями, присвоения, растраты или использования компьютерной техники. Кроме того, криминообразующие признаки отдельных видов хищения путем использования компьютерной техники встречаются при охране иных, кроме собственности, групп общественных отношений. Так, УК Беларуси устанавливает ответственность за некоторые виды хищения с использованием информационных технологий в группе преступлений против общественной безопасности (гл. 27). Здесь выделяется умышленное противоправное безвозмездное завладение огнестрельным оружием, боеприпасами или взрывчатыми веществами либо правом на них путем использования компьютерной техники независимо от наличия или отсутствия корыстной цели (ст. 294). Отдельные виды хищений, совершенных с использованием компьютерной техники, УК Беларуси закрепляет в гл. 29 «Преступления против здоровья населения». В частности, в примечании к этой главе оговаривается, что под хищениями радиоактивных материалов (ст. 323), наркотических средств, психотропных веществ, их прекурсоров и аналогов (ст. 327), сильнодействующих или ядовитых веществ (ст. 333) понимается умышленное противоправное безвозмездное завладение указанными материалами, средствами, препаратами, веществами или правом на них путем использования компьютерной техники независимо от наличия или отсутствия корыстной цели.

Непосредственно ответственность за хищение путем использования компьютерной техники предусматривается в ст. 212 УК Беларуси. Принимая во внимание дефиницию хищения, изложенную в примечании 1 к гл. 24 УК Беларуси, и содержание ст. 212 УК Беларуси, под хищением путем использования компьютерной техники следует понимать умышленное противоправное безвозмездное завладение чужим имуществом или правом на имущество с корыстной целью, совершенное путем: 1) изменения информации, обрабатываемой в компьютерной системе, хранящейся на машинных носителях или передаваемой по сетям передачи данных (путем обманного использования в корыстных целях ошибки компьютерного обеспечения в результате присвоения имени пользователя, персонального идентификационного номера и использования их в качестве электронной подписи при совершении операций посредством компьютерной техники²⁷, существенного видоизменения пер-

²² См.: Серебренникова А. В. Особенная часть. Уголовное право ФРГ // Уголовное право зарубежных стран. Общая и Особенная части: учебник для магистров / под ред. Н. Е. Крыловой. 4-е изд. М., 2013. С. 892—894.

²³ См.: Жалинский А. Э. Современное немецкое уголовное право. М., 2004. С. 462—463.

²⁴ См.: Janke G. Kompendium Wirtschaftskriminalität. Peter Lang GmbH International Verlag der Wissenschaften. Frankfurt am Main, 2008. S. 231—232.

²⁵ См.: Власов И. С., Голованова Н. А., Меньших А. А. Указ. соч. С. 130.

²⁶ См.: Janke G. Op. cit. S. 232—237.

²⁷ См., например, приговор суда г. Новополоцка от 26 января 2015 г. по уголовному делу по обвинению жителя Новополоцка, работавшего оператором производства на ОАО «Нафтан», в совершении преступления, предусмотренного ч. 4 ст. 212 УК Республики Беларусь. URL: http://court.by/justice/press_office/e1d29d938dba8956.html.

воначального содержания компьютерной информации, внесения различных корректировок в уже существующую информацию, затрудняющих ее законное использование); 2) введения в компьютерную систему ложной информации (посредством внесения любых не соответствующих действительности данных (создания новой информации), отличных от тех, которые были введены в систему собственником информационного ресурса²⁸); 3) совершения этих же деяний, сопряженных с несанкционированным доступом к компьютерной информации (незаконное перечисление денежных средств с помощью поддельных банковских карт со счетов иностранных банков, введения в компьютерные системы интернет-магазинов, процессинговых центров банков-эмитентов, банков-эквайеров, платежных систем неправомерно полученной конфиденциальной информации о проведении операций по оплате товарно-материальных ценностей (услуг) от имени держателей банковских персональных карт без их разрешения и согласия, не имея на то действительного и предполагаемого права²⁹).

Разъясняя вопросы квалификации, Пленум Верховного суда Республики Беларусь в абз. 1 п. 20 постановления от 21 декабря 2001 г. № 15 «О применении судами уголовного законодательства по делам о хищениях имущества» подчеркнул, что хищение путем использования компьютерной техники (ст. 212 УК Беларуси) может совершаться лишь посредством тех компьютерных манипуляций, которые состоят в обмане потерпевшего или иного лица, которому имущество было вверено либо под охраной которого оно находится, с использованием системы обработки информации. При отсутствии таких признаков, но в случае извлечения имущественных выгод в результате модификации компьютерной информации и причинения имущественного ущерба в значительном размере (например, при использовании идентификационных номеров легальных пользователей без цели оплаты услуг сотовых операторов) деяние надлежит квалифицировать как причинение имущественного ущерба без признаков хищения (ст. 216 УК Беларуси).

Исходя из буквального толкования примечания 1 к гл. 24 УК Беларуси, хищение путем использования

компьютерной техники (ст. 212) не является частным случаем кражи (ст. 205) или мошенничества (ст. 209). В частности, в руководящих разъяснениях Верховного суда однозначно констатируется: «В отличие от мошенничества при хищении путем использования компьютерной техники, завладение имуществом происходит посредством использования компьютерной техники. Если лицо при помощи компьютерной техники изготовило фиктивный документ, а затем использовало его для завладения имуществом путем обмана, все содеянное квалифицируется как мошенничество»³⁰. Следовательно, при квалификации хищения путем использования компьютерной техники должно учитываться воздействие не на человека, а на результат автоматизированной обработки данных, совершенное в целях завладения чужим имуществом (манипулирование компьютерной информацией), непосредственно приведшее к его хищению³¹.

В отличие от УК Беларуси в Уголовном кодексе Республики Узбекистан от 22 сентября 1994 г. № 2012-XII нормы об ответственности за хищения, совершенные с использованием компьютерной техники либо сопряженные с несанкционированным проникновением в компьютерную систему, сконцентрированы только в одной главе Особенной части Кодекса — гл. X «Хищение чужого имущества» — и включены в квалифицирующие признаки лишь трех форм хищения: присвоения или растраты (п. «г» ч. 3 ст. 167), мошенничества (п. «г» ч. 2 ст. 168) и кражи (п. «б» ч. 3 ст. 169).

Вопросы, возникающие в судебной практике при разграничении этих форм хищения, разрешены в постановлении Пленума Верховного суда Республики Узбекистан от 24 июля 2009 г. № 8 «О судебной практике по делам о мошенничестве». Например, в абз. 2 п. 10 постановления содержится четкое указание о разграничении мошенничества и кражи в системе дистанционного банковского обслуживания, согласно которому под признаки кражи чужого имущества подпадает хищение чужих денежных средств путем использования похищенной (поддельной) кредитной либо расчетной карты, если выдача наличных денежных средств осуществлена посредством банкомата. Вместе с тем как мошенничество может быть квалифицировано хищение чужих денежных средств, находящихся на счетах в банках, путем использования похищенной (поддельной) кредитной либо расчетной карты в случаях, когда лицо путем обмана или злоупотребления доверием ввело в заблуждение уполномоченного работника кредитной, торговой или

²⁸ Подробнее см.: Хилута В. В. Квалификация преступлений против собственности. Гродно, 2013.

²⁹ См., например, приговор суда Ленинского района г. Могилева Республики Беларусь от 21 августа 2015 г. по уголовному делу по обвинению С. в совершении преступлений, предусмотренных ч. 1 ст. 14, ч. 4 ст. 212, ч. 2 ст. 235, ст. 352 УК Республики Беларусь. URL: http://court.by/justice/press_office/ccf9fbb458bb907f.html; приговор суда Бобруйского района и г. Бобруйска Могилевской области Республики Беларусь от 16 ноября 2015 г. по уголовному делу по обвинению жителя Бобруйска в совершении преступлений, предусмотренных ч. 4 ст. 212, ч. 2 ст. 349, ст. 352 УК Республики Беларусь. URL: http://court.by/justice/press_office/d0edd4170ead0089.html.

³⁰ Пункт 22 постановления Пленума Верховного суда Республики Беларусь от 21 декабря 2001 г. № 15 «О применении судами уголовного законодательства по делам о хищениях имущества».

³¹ См.: Хилута В. В. Квалификация преступлений против собственности.

сервисной организации (например, используя банковскую карту для оплаты товаров или услуг в торговом или сервисном центре, лицо ставит подпись в чеке на покупку вместо законного владельца карты либо предъявляет поддельный паспорт на его имя).

3. В уголовном законодательстве ряда зарубежных государств понятие «компьютерные технологии», во-первых, отождествляется с предметом киберпреступлений и, во-вторых, признается одним из способов и средств совершения различных видов преступлений — в сфере экономической деятельности, против свободы, чести и достоинства личности, здоровья населения и общественной нравственности, основ конституционного строя и безопасности государства (Великобритания, Белоруссия, Киргизия, Таджикистан).

В *Великобритании*, например, в Законе о телекоммуникациях (обманах) 1997 г. предусмотрена ответственность за владение и поставку другим лицам предметов в целях обманного получения закрытой информации путем использования телекоммуникационной системы (ст. 1(6)) — оборота предметов, применяемых для записи любых данных, последующего использования этих данных с намерением бесчестного получения услуг. Законом о серьезной преступности 2015 г. Закон о неправомерном использовании компьютерных технологий 1990 г. был дополнен положениями об умышленных и неосторожных несанкционированных действиях с компьютером, которые причиняют либо создают угрозу причинения серьезного материального вреда (ст. 41—44).

Установление в законодательстве государств — участников СНГ уголовной ответственности за использование информационных технологий в качестве способа совершения преступлений движется по нескольким направлениям. В одном случае уголовное законодательство тяготеет к тенденции закрепления критерия использования информационных технологий в числе признаков объективной стороны тех или иных составов преступлений, посягающих на сферу экономической деятельности. Наиболее наглядным в этой области видится законодательный опыт Киргизии и Таджикистана. Например, Уголовный кодекс *Кыргызской Республики* от 1 октября 1997 г. № 68 к преступлениям в сфере экономической деятельности (гл. 22) относит собирание сведений, составляющих коммерческую или банковскую тайну, путем незаконного проникновения в компьютерную систему или сеть, использования специальных технических средств в целях разглашения либо использования этих сведений (ст. 193). Аналогичная норма содержится в главе о преступлениях в сфере экономической деятельности Уголовного кодекса *Республики Таджикистан* от 21 мая 1998 г. № 574 (ст. 277 гл. 27). Уголовный кодекс *Республики Казахстан* от 3 июля 2014 г. № 226-V ЗРК признает уголовно наказуемым сбор сведений, составляющих коммерческую или банковскую тайну, а также информации, связан-

ной с проведением процедуры легализации имущества, путем незаконного проникновения в компьютерную систему или сеть, использования специальных технических средств (ч. 1 ст. 223 гл. 8). Отметим, что в ст. 183 УК РФ подобная конкретизация способа незаконного получения и разглашения сведений, составляющих коммерческую, налоговую или банковскую тайну, отсутствует. Совершение этого деяния путем использования информационных технологий составляет «иной незаконный способ» собирания соответствующих сведений.

В другом случае использование кибертехнологий признается способом и средством совершения ряда других преступлений, имеющих иной видовой объект. Например, в УК *Таджикистана* подделка, изготовление или сбыт поддельных документов, государственных наград, штампов, печатей, бланков с использованием компьютерной техники признается преступлением против порядка управления (п. «в» ч. 2 ст. 340 гл. 31). Уголовный кодекс *Туркменистана* от 12 июня 1997 г. № 222-1 в число преступлений против основ конституционного строя и безопасности государства (гл. 22) включает получение незаконным путем государственных секретов, их разглашение и распространение путем незаконного проникновения в компьютерную систему или сеть, использования специальных технических средств (ст. 179), а также утрату документов, содержащих государственные секреты, если такая утрата явилась результатом нарушения установленных правил хранения компьютерных сведений (ст. 180). В некоторой степени схожее обстоятельство закрепляется и в п. «г» ч. 2 ст. 283¹ УК РФ об ответственности за незаконное получение сведений, составляющих государственную тайну, совершенное с использованием специальных и иных технических средств, предназначенных для негласного получения информации. По аналогии с УК РФ (п. «б» ч. 3 ст. 242¹, п. «г» ч. 2 ст. 242²) УК *Беларуси* в главе о преступлениях против общественного порядка и общественной нравственности (гл. 30) устанавливает ответственность за использование глобальной компьютерной сети Интернет, иной сети электросвязи общего пользования либо выделенной сети электросвязи для изготовления и распространения порнографических материалов или предметов порнографического характера (ч. 2 ст. 343), в том числе с изображением несовершеннолетнего (ч. 2 ст. 343¹). Кроме того, к преступлениям против личной свободы, чести и достоинства личности относится клевета, содержащаяся в информации, размещенной в глобальной компьютерной сети Интернет (гл. 22 ч. 2 ст. 188 УК Беларуси).

4. Еще одной тенденцией развития уголовно-правовых мер противодействия киберпреступности в законодательстве зарубежных стран является конструирование в уголовном законодательстве зарубежных стран норм, в настоящее время не свойственных для УК РФ. В качестве примера можно привести: регла-

ментацию уголовной ответственности за фальсификацию компьютерной информации (ст. 273² Уголовного кодекса Азербайджанской Республики от 30 декабря 1999 г. № 787-IQ, ст. 260⁶ УК Молдовы); компьютерный саботаж (ст. 351 УК Беларуси, ст. 300 УК Таджикистана, ст. 278⁵ УК Узбекистана); незаконный оборот средств, изготовленных для совершения киберпреступлений (ст. 273¹ УК Азербайджана); принуждение к передаче охраняемой законом информации, хранящейся на электронном носителе, содержащейся в информационной системе или передаваемой по сетям телекоммуникаций, под угрозой применения насилия либо уничтожения или повреждения имущества, распространения сведений, позорящих потерпевшего или его близких (ст. 209 УК Казахстана); предоставление услуг для размещения интернет-ресурсов, преследующих противоправные цели (ст. 212 УК Казахстана).

В русле этой тенденции интерес представляют подходы законодателей зарубежных стран к так называемому распиливанию признаков неправомерного доступа к компьютерной информации на самостоятельные составы преступления путем конкретизации в них общественно опасных последствий. Как известно, в соответствии со ст. 272 УК РФ ответственность за неправомерный доступ к охраняемой законом компьютерной информации возможна только в случае наступления в результате этого деяния последствий в виде уничтожения, блокирования, модификации либо копирования компьютерной информации. Вместе с тем в уголовном законодательстве родственных нам по правовой системе государств — участников СНГ ответственность за модификацию компьютерной информации устанавливается в отдельных нормах. Например, в УК *Беларуси* регламентируется ответственность за изменение информации, хранящейся в компьютерной системе, сети или на машинных носителях, либо внесение заведомо ложной информации, причинившие существенный вред, при отсутствии признаков преступления против собственности (ст. 350); в УК *Казахстана* — за умышленные неправомерные уничтожение или модификацию охраняемой законом информации, хранящейся на электрон-

ном носителе, содержащейся в информационной системе или передаваемой по сетям телекоммуникаций, а равно ввод в информационную систему заведомо ложной информации, если это повлекло существенное нарушение прав и законных интересов граждан или организаций либо охраняемых законом интересов общества или государства (ст. 206); в УК *Таджикистана* — за изменение информации, хранящейся в компьютерной системе, сети или на машинных носителях, а равно внесение в них заведомо ложной информации, причинившие значительный ущерб или создавшие угрозу его причинения (ст. 299); в УК *Узбекистана* — за изменение, повреждение, стирание информации, хранящейся в компьютерной системе, а равно внесение в нее заведомо ложной информации, причинившие крупный ущерб либо существенный вред правам или охраняемым законом интересам граждан либо государственным или общественным интересам (ст. 278⁴).

Подводя итог компаративистскому анализу уголовно-правовых мер противодействия киберпреступлениям за рубежом, следует отметить, что, безусловно, подход к криминализации деяний, посягающих на информационную безопасность, в уголовном законодательстве каждого государства нельзя признать идентичным, он различен и в определении объекта преступления, и в установлении видов деяний, и в закреплении способов совершения таких посягательств. Однако имеется в таком подходе и неотъемлемая тождественность. Сегодня «окраска» общественной опасности посягательств на информационную безопасность изменилась, она вышла за рамки только одной группы уголовно-правовых норм — экономической и информационной направленности. Стремительное развитие кибертехнологий предопределило необходимость криминализации их использования в качестве способов, средств либо криминообразующих признаков многих деяний, нарушающих иные общественные отношения, — конституционные права и свободы личности, интересы собственности, сферу экономической деятельности, здоровье населения и общественную нравственность, конституционный строй и безопасность государства.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

- Ashworth A. J. United Kingdom // *The Handbook of Comparative Criminal Law* / eds. by K. J. Heller, M. D. Dubber. Stanford; California, 2011.
- Bronitt S., McSherry B. *Principles of Criminal Law*. 3rd ed. Sydney, 2006.
- Computer and Internet Fraud // Cornell University Law School. Legal Information Institute. URL: http://www.law.cornell.edu/wex/computer_and_internet_fraud.
- Federal Criminal Law and its Enforcement / N. Abrams, S. Sun Beale, S. R. Klein. 5th ed. West, 2010.
- Identity Theft (FAQ) // Nolo. Law for All. URL: <http://www.nolo.com/legal-encyclopedia/identity-theft-faq-29074.html>.
- Janke G. *Kompendium Wirtschaftskriminalität*. Peter Lang GmbH International Verlag der Wissenschaften. Frankfurt am Main, 2008.
- Mazzone A. Identity Fraud — Government Legislative Responses // Victorian Government Solicitor's Office. URL: <http://vgso.vic.gov.au/sites/default/files/publications/Identity%20Fraud%20-%20Government%20Legislative%20Responses.pdf>.
- Odenthal R. *Korruption und Mitarbeiterkriminalität: Wirtschaftskriminalität vorbeugen, erkennen und aufdecken*. 2., vollständig überarbeitete und erweiterte Auflage. Gabler | GWV Fachverlage GmbH, Wiesbaden, 2009.

What is Illegal under Local, State and Federal Laws? Federal Computer Security Violations // Cornell University. IT Cornell. URL: <http://www.it.cornell.edu/policies/university/privacy/responsible/illegal.cfm>.

Власов И. С., Голованова Н. А., Меньших А. А. Ответственность за компьютерные преступления по законодательству зарубежных государств // Журнал зарубежного законодательства и сравнительного правоведения. 2005. № 2.

Голованова Н. А. Особенная часть. Уголовное право Англии // Уголовное право зарубежных стран. Общая и Особенная части: учебник / под ред. И. Д. Козочкина. 3-е изд. М., 2010.

Гришук-Бучка С. Уголовно-правовая характеристика преступлений против компьютерной безопасности (по законодательству Республики Молдова). URL: <http://security.ase.md/materials/si2010/material-2010.pdf>.

Дмитришен М., Гончаров И. Мошенничество в информационных технологиях. URL: <http://security.ase.md/>.

Жалинский А. Э. Современное немецкое уголовное право. М., 2004.

Маймеску С. Глава XXI. Информационные преступления и преступления в области электросвязи // Комментарий к Уголовному кодексу Республики Молдова. Общая и Особенная части. Кишинэу, 2010.

Семыкина О. И. Тенденции борьбы с преступлениями в сфере информационных технологий (сравнительно-правовой аспект) // Сборник трудов XXIII Всероссийской конференции «Информатизация и информационная безопасность правоохранительных органов». М., 2014.

Серебренникова А. В. Особенная часть. Уголовное право ФРГ // Уголовное право зарубежных стран. Общая и Особенная части: учебник для магистров / под ред. Н. Е. Крыловой. 4-е изд. М., 2013.

Сидоренко Э. Л., Волеводз А. Г. Мошенничество в сфере предпринимательской деятельности: особенности судебного толкования // Мировой судья. 2016. № 2.

Сидоренко Э. Л. Мошенничество в сфере страхования: некоторые проблемы квалификации // Уголовное право. 2015. № 5.

Хилjuta В. В. Квалификация преступлений против собственности. Гродно, 2013.

Хилjuta В. В. Уголовная ответственность за хищения с использованием компьютерной техники // Журнал российского права. 2014. № 3.