ристик, принимая во внимание уровень ущерба, который они причинили своими преступными действиями экономике государства, в том числе банкротством вверенных им предприятий, а в ряде случаев и потерей доверия людей к исполнительной и распорядительной власти.

1. Долгова, А.И. Личность преступника / А.И. Долгова // Российская криминологическая энциклопедия: преступность и борьба с ней в понятиях и комментариях / под общ. ред. А.И. Долговой. – М., 2000. – С. 321–322.

2. Антонян, Ю.М. Личность преступника = Personality of criminal / Ю.М. Антонян, В.Н. Кудрявцев, В.Е. Эминов. – СПб. : Юрид. центр Пресс, 2004. – 364 с.

3. Иншаков, С.М. Криминология: вопросы и ответы : учеб. пособие / С.М. Иншаков. – М. : Юриспруденция, 2000. – 215 с.

4. Получение взятки муниципальными служащими: уголовно-правовые и криминологические аспекты : монография / В.Д. Ларичев [и др.]. – М. : Юрлитинформ, 2012. – 296 с.

5. Гладков, А.В. Криминологическая характеристика осужденного коррупционера (на примере ИК-19 УДИН МВД Республики Беларусь по Могилевской области) / А.В. Гладков // Исполнение уголовных наказаний и иных мер уголовной ответственности : материалы Междунар. науч.-практ. конф., Минск, 22 апр. 2010 г. / Акад. М-ва внутр. дел Респ. Беларусь ; редкол.: А.В. Шарков (отв. ред.) [и др.]. – Минск, 2010. – С. 103–106.

Дата поступления в редакцию: 01.03.17

***V.S. Gladkov**, Postgraduate student of the Scientific and Pedagogical Faculty of the Academy of the MIA of the Republic of Belarus*

TYPOLOGY OF THE IDENTITY OF THE OFFENDER-CORRUPT

Analyzes the results of the empirical study carried out by the author among persons convicted of committing corruptive crimes, and also suggests the typology of the personality of the offender of corruption oriented on the basis of it.

Keywords: personality typology, personal characteristics, personality of the corrupt criminal, characterization of the person, punishment, corruption.

УДК 340

***М.А. Дубко**, следователь по особо важным делам управления анализа практики и методического обеспечения предварительного расследования центрального аппарата Следственного комитета (e-mail: mihail-dubko@tut.by)*

ОСНОВАНИЕ И ПРИЧИНЫ КРИМИНАЛИЗАЦИИ НЕПРАВОМЕРНОГО ЗАВЛАДЕНИЯ КОМПЬЮТЕРНОЙ ИНФОРМАЦИЕЙ

Рассматриваются социально-правовые причины установления в Республике Беларусь уголовной ответственности за неправомерное завладение компьютерной информацией, основание криминализации данного деяния, по результатам чего автором сделан ряд выводов. В частности, сформулировано определение основания криминализации неправомерного завладения компьютерной информацией, предложен теоретический подход к установлению уголовной ответственности за деяния, связанные с противоправным получением информации, предложено декриминализировать несанкционированное копирование компьютерной информации как один из способов неправомерного завладения компьютерной информацией и рассматривать его в рамках состава несанкционированного доступа.

Ключевые слова: завладение компьютерной информацией, несанкционированное копирование, основание криминализации, общественная опасность.

Развитие информационного общества в республике является одним из национальных приоритетов. Вопросы защиты компьютерной информации приобретают особую актуальность в рамках реализации Программы социально-экономического развития Республики Беларусь на 2016–2020 годы, а также Государственной программы инновационного развития Республики Беларусь на 2016–2020 годы.

Сфера правовой защиты компьютерной информации содержит и уголовно-правовые средства, позволяющие обеспечить предупреждение наиболее опасных посягательств на информационную безопасность, к числу которых законодателем отнесено неправомерное завладение компьютерной

информацией (ст. 352 УК). Проблемные аспекты уголовной ответственности за неправомерное завладение компьютерной информацией не нашли достаточного отражения в исследованиях белорусских ученых и требуют дальнейшей глубокой проработки. В связи с указанным видится необходимым вернуться к рассмотрению вопросов основания и причин криминализации данного деяния.

Распространение и применение в 90-е гг. XX в. компьютерных технологий привели к возникновению новых отношений, которые не укладывались в рамки существующих правовых институтов [1, с. 7], изменению характера и появлению новых видов преступлений, что, по мнению А.Ж. Кабановой, стало исторической предпосылкой их криминализации [2, с. 7] . Ученые, анализируя состояние компьютерной преступности в других государствах, приводили данные о значительном росте ущерба в результате совершения компьютерных преступлений [3, с. 12–13; 4, с. 18–19].

Так, В.С. Комиссаров указывал, что «несанкционированные действия по уничтожению, модификации, копированию информации… способны вызвать тяжкие и необратимые последствия, связанные не только с имущественным ущербом, но и с физическим вредом людям» [5, с. 9]. Еще в 1991 г. Ю.М. Батурин обращал внимание на то, что «информация имеет ценность для собственника до тех пор, пока он является ее монопольным владельцем» [6, с. 26], в связи с чем предложил отнести хищение информации к преступлению. В.С. Бондаренко, наоборот, отмечал, что «для социалистических стран такие явления не характерны» [7, с. 4]. По мнению Н.Ф. Ахраменка, в данный период следовало провести превентивную криминализацию до того, как общественно опасные действия с использованием информационно-вычислительных систем получат реальную массовую распространенность [8, л. 35–36]. Ученый писал: «Учитывая потенциальную опасность использования электронно-вычислительной техники..., следует обеспечить опережающую разработку нормативной правовой базы защиты личности, общества и государства от отрицательных социальных последствий информатизации» [9, с. 8]. В этой связи включение в белорусский уголовный закон ст. 349–355, предусматривающих ответственность за преступления против информационной безопасности, явилось «превентивной» мерой защиты данных отношений. Корректировка уголовного закона в данной части обусловлена в большей степени развитием международного и зарубежного законодательств.

После вступления УК в силу специалисты указывали на необходимость разработки нормативного правового акта, который бы регулировал «отношения, связанные с созданием и использованием различных современных средств коммуникаций и обеспечивал защиту прав владельцев электронной информации в этих сетях» [10, с. 10]. Однако, наоборот, в ключевом законодательном акте, определяющем основы отношений в информационной сфере, закреплено, что информация есть сведения независимо от формы представления.

Как отмечает С.А. Чернышева, необходимыми условиями правовой защиты компьютерной информации одновременно являются: наличие правовых норм, в соответствии с требованиями которых должны строиться отношения между людьми по поводу сбора, накопления, хранения и использования компьютерной информации, и определение юридической ответственности за несоблюдение должного поведения [11, с. 20]. Нормы, образующие состояние противоправности, имеют «определяющее значение для существования юридической ответственности за противоправные деяния в информационной сфере» [12, с. 20].

На основании изложенного видится незавершенным этап закрепления уголовной ответственности за преступления против информационной безопасности. Для обеспечения полноты и комплексности правового регулирования требуется принятие отдельного законодательного акта либо внесение изменений в действующий закон о защите информации, урегулировавших бы отношения, возникающие в процессе создания, распространения, использования, хранения и уничтожения компьютерной информации. Тем самым была бы обеспечена связь норм, предусматривающих юридическую ответственность, с системой дозволений, запретов, ограничений и стимулов, которые формируют правовой режим в информационной среде [12, с. 8–9].

Анализ национального информационного законодательства показал, что правовой режим информации есть характеристика информации как объекта правоотношений, вытекающая из ее нематериальной природы, а требования к защите информации определяются ее содержанием, а не формой представления. Данный вывод соотносится с тезисом о том, что «в информационном обществе приоритетное значение приобретает проблема регулирования информации как таковой, не привязанной к специфике своего материального носителя и форме ее представления» [13, с. 10]. Сходной позиции придерживается И.Ю. Богдановская, отмечая, что различные ограничения в отношении информации связаны прежде всего с ее содержанием [14, с. 59].

С учетом сказанного при правовом регулировании информации, в том числе при установлении ответственности, первичным должен являться социальный признак, заключающийся в ее «общественной значимости для удовлетворения различных потребностей и (или) интересов индивидов, коллективов, социальных общностей, юридических лиц и государственных органов» [15, с. 41].

Так, система уголовно-правовых норм, предусматривающих ответственность за так называемые информационные преступления, в УК 1960 г. (ст. 61, 62, 72, 73, 122[1], 135, 138, 248 и др.), УК 1999 г. (ст. 177–179, 203, 254, 358, 407 и др.) выстраивалась на основе указанных принципов. В этой связи представляется, что включение в УК ст. 349–355, предметом которых является информация по признаку формы представления (компьютерная информация), закономерно вызывает сложности в определении их места в системе уголовного закона и трудности в правоприменении.

Общественная опасность – важнейшее свойство преступления, отличающее его от иных видов правонарушений и обусловливающее необходимость уголовно-правового запрета [16, с. 1]. Не подвергая сомнению общественную опасность деяния как основание установления уголовно-правового запрета (Г.Ю. Лесников, Н.А. Лопашенко, А.В. Наумов, П.С. Тоболкин, Т.Г. Хатеневич и др.), важно обратить внимание на необходимость соблюдения законодателем социально-правового принципа криминализации – неизбыточности запрета [17, с. 215–242; 18, с. 108], который должен выражаться в том числе в невозможности применения к новым общественным отношениям имеющихся уголовно-правовых норм, их неэффективности.

Так, А.Э. Жалинский к перечню обязательных требований, достаточных для признания общественной опасности поведения, подлежащего уголовно-правовому запрету, относил «доказанную непригодность иных правовых запретов для устранения возникшей опасности, возмещения причиненного и предупреждения потенциального вреда» [19, с. 52]. По мнению Г.А. Злобина [17, с. 241], необходимость воздействия на общественные отношения уголовно-правовыми мерами и соответственно потребность в криминализации деяния имеется только в случае отсутствия нормы, достаточно эффективно регулирующей соответствующие отношения.

Встраивание нового объекта в существующую правовую систему возможно посредством нескольких вариантов: когда к объекту с учетом его свойств и характеристики можно в полной мере применить уже существующие нормы, правовые институты; когда для нового объекта создаются специальные нормы, предназначенные для этого объекта, учитывающие его правовую природу и свойства [1, с. 24]. Изложенные способы в полной мере применимы к нормотворческому процессу по включению в уголовный закон норм гл. 31. Однако несмотря на то, что уголовный закон (аналогично УК 1960 г.) содержит целый ряд составов преступлений, предусматривающих ответственность за различные формы противоправного получения (похищение, собирание) информации исходя из ее содержания (банковская тайна, государственные секреты, тайна личной жизни и др.), при криминализации неправомерного завладения компьютерной информации (ст. 352 УК) законодатель избрал последний вариант.

В этой связи общественная опасность неправомерного завладения компьютерной информацией как основание его криминализации должна выражаться в свойстве данного деяния причинить или создать реальную угрозу причинения вреда охраняемым уголовным законом отношениям и интересам посредством несанкционированного копирования или иного неправомерного завладения компьютерной информацией безотносительно установленного в отношении ее правового режима. Предлагаемое определение раскрывает сущность уголовно-правового запрета, изложенного в ст. 352 УК, и способствует точному определению его признаков. Так, например, к последствиям неправомерного завладения компьютерной информацией (существенному вреду), не связанным с причинением имущественного вреда, следует относить: изменение, уничтожение, блокирование информации, вывод из строя либо нарушение работы компьютерного оборудования, остановку производственного процесса автоматизированного предприятия, прекращение функционирования информационной системы или сети электросвязи, невозможность полноценного осуществления государственным органом или иной организацией своих функций и др., т. е. такие последствия, наступление которых обусловлено компьютерной формой информации.

Согласно изложенному предлагается теоретический подход к установлению уголовной ответственности за общественно опасные деяния, связанные с противоправным получением (похищением, собиранием, завладением) информации, в основе которого следующие положения:

1) при криминализации деяний, связанных с противоправным получением информации, необходимо исходить из содержания информации как предмета преступления и соответственно

возможности наступления негативных последствий в случае противоправного обладания ею, что обусловливает общественную опасность деяния;

2) необходимо установление повышенной ответственности за противоправное получение информации, хранящейся в компьютерной системе, сети, на машинных носителях либо передаваемой с использованием средств компьютерной связи, в составах преступлений, предметом которых является информация безотносительно формы ее представления;

3) следует сохранить в гл. 31 УК нормы, предусматривающие уголовную ответственность только за такие способы противоправного получения компьютерной информации, которые способны причинить или создать реальную угрозу причинения вреда охраняемым уголовным законом отношениям и интересам безотносительно установленного в отношении ее правового режима. К таковым необходимо отнести только завладение компьютерной информацией, под которым предлагается понимать умышленные действия лица по получению компьютерной информации, в том числе путем перехвата, в результате чего обладатель информации либо ее получатель лишаются возможности использовать данную информацию.

Так, анализ объективных признаков состава неправомерного завладения компьютерной информацией выявил диспропорцию в степени общественной опасности альтернативных деяний (несанкционированное копирование, иное неправомерное завладение) в рамках одного состава. В отсутствие иных признаков состава преступления, предусмотренного ст. 352 УК, характеризующих предмет преступления, объективную или субъективную сторону и повышающих степень общественной опасности деяния, целесообразной является декриминализация несанкционированного копирования компьютерной информации как одного из способов неправомерного завладения компьютерной информацией, изложенного в ст. 352 УК. С учетом сходности непосредственного объекта двух преступлений (несанкционированное копирование и несанкционированный доступ), а также результата данных противоправных деяний предлагается в правоприменительной деятельности действия по несанкционированному копированию компьютерной информации рассматривать в рамках несанкционированного доступа как признака преступления, предусмотренного ст. 349 УК.

Таким образом, предлагается:

определение общественной опасности неправомерного завладения компьютерной информацией как основания его криминализации, которое раскрывает сущность уголовно-правового запрета, изложенного в ст. 352 УК, а также способствует точному определению признаков данного состава и соответственно правильной юридической оценке общественно опасных деяний, связанных с противоправным получением информации (ст. 179, 254, 352, 358 УК и др.);

теоретический подход к установлению уголовной ответственности за общественно опасные деяния, связанные с противоправным получением информации, включающий в том числе предложение о декриминализации несанкционированного копирования компьютерной информации как одного из способов неправомерного завладения компьютерной информацией, изложенного в ст. 352 УК. Реализация данного подхода при дальнейшем совершенствовании уголовного закона в части установления уголовной ответственности за противоправное завладение различными видами информации обеспечит его системность, исключит проблемные вопросы квалификации таких деяний, будет соотноситься с развитием национального информационного законодательства.

1. Терещенко, Л.К. Правовой режим информации : автореф. дис. ... д-ра юрид. наук : 12.00.14 / Л.К. Терещенко. – М., 2011. – 54 с.

2. Кабанова, А.Ж. Преступления в сфере компьютерной информации (уголовно-правовые и криминологические аспекты) : автореф. дис. … канд. юрид. наук : 12.00.08 / А.Ж. Кабанова. – Роснов н/Д., 2004. – 28 с.

3. Черкасов, В.Н. Компьютерная преступность и ее предупреждение : учеб.-метод. пособие / В.Н. Черкасов. – Минск, 1994. – 76 с.

4. Вехов, В.Б. Компьютерные преступления: способы совершения и методы расследования / В.Б. Вехов ; под ред. Б.П. Смагоринского. – М. : Право и закон, 1996. – 182 с.

5. Комиссаров, В.С. Преступления в сфере компьютерной информации: понятие и ответственность / В.С. Комиссаров // Юрид. мир. – 1998. – № 2. – С. 9–19.

6. Батурин, Ю.М. Компьютерная преступность и компьютерная безопасность / Ю.М. Батурин, А.Н. Жодзишский. – М. : Юрид. лит., 1991. – 157 с.

7. Бондаренко, В.С. Сохранность информации при автоматизированной обработке / В.С. Бондаренко. – М. : Знание, 1981. – 64 с.

8. Ахраменка, Н.Ф. Проблемы криминализации общественно опасного поведения с использованием информационно-вычислительных систем : дис. … канд. юрид. наук : 12.00.08 / Н.Ф. Ахраменка ; Белорус. гос. ун-т. – Минск, 1996. – 122 л.

9. Ахраменка, Н.Ф. Проблемы криминализации общественно опасного поведения с использованием информационно-вычислительных систем : автореф. дис. … канд. юрид. наук : 12.00.08 / Н.Ф. Ахраменка ; Белорус. гос. ун-т. – Минск, 1996. – 19 с.

10. Рыжевский, А.В. Состояние законодательства Республики Беларусь в области безопасности информации / А.В. Рыжевский // Компьютерные технологии в обеспечении безопасности электронной информации : материалы Междунар. конф. – Минск : БелИСА, 2002. – С. 5–11.

11. Чернышева, С.А. Правовая информатика : курс лекций / С.А. Чернышева, А.Г. Шипулина. – Минск : БИП-С Плюс, 2011. – 212 с.

12. Полушкин, А.В. Информационные правонарушения: понятие и виды : автореф. дис. … канд. юрид. наук : 12.00.14 / А.В. Полушкин. – Екатеринбург, 2009. – 26 с.

13. Войникалис, Е.А. Информация. Собственность. Интернет. Традиция и новеллы в современном праве / Е.А. Войникалис, М.В. Якушев. – М. : Волтерс Клувер, 2004. – 176 с.

14. Право на доступ к информации. Доступ к открытой информации / отв. ред. И.Ю. Богдановская. – М. : Юстицинформ, 2009. – 344 с.

15. Мороз, Л.Н. Информационное право. Общая часть / Л.Н. Мороз. – Минск : Право и жизнь, 2007. – 276 с.

16. Пермяков, Ю.Е. Категория «общественная опасность» в советском уголовном праве : автореф. дис. ... канд. юрид. наук : 12.00.08 / Ю.Е. Пермяков. – М., 1989. – 23 с.

17. Основания уголовно-правового запрета. Криминализация и декриминализация / П.С. Дагель [и др.] ; отв. ред. В.Н. Кудрявцев, А.М. Яковлев. – М. : Наука, 1982. – 303 с.

18. Лопашенко, Н.А. Уголовная политика / Н.А. Лопашенко. – М. : Юрлитинформ, 2009. – 176 с.

19. Жалинский, Э.А. Оценка общественной опасности деяния в процессе уголовного правотворчества / Э.А. Жалинский // Уголовное право: стратегия развития в XXI веке : материалы 6-й Междунар. науч.-практ. конф., Москва, 29–30 янв. 2009 г. – М., 2009. – С. 48–52.

Дата поступления в редакцию: 03.04.17

***M.A. Dubko**, Investigator (serious crime), Investigative Committee of the Republic of Belarus*

THE REASONS OF THE CRIMINALIZATION OF COMPUTER INFORMATION MISAPPROPRIATION

The article deals socio-legal reasons for establishing criminal liability for the misappropriation of computer information in the Republic of Belarus, which resulted in the author making a number of conclusions. In particular, the definition of the reasons of the criminalization of the computer information misappropriation was formulated, a theoretical model to criminal liability for acts connected with information misappropriation was proposed, and it was suggested to decriminalize unauthorized copying of computer information.

Keywords: reasons of criminalization, misappropriation of computer information, unauthorized copying of computer information, public danger.

УДК 343.914

***М.Ю. Кашинский**, кандидат юридических наук, доцент, начальник научно-педагогического факультета Академии МВД Республики Беларусь*
(e-mail: m.kashinsky@yandex.ru);
***Ю.Ф. Машталер**, адъюнкт научно-педагогического факультета Академии МВД Республики Беларусь*
(e-mail: y_f_mashtaler@mail.ru)

КРИМИНОЛОГИЧЕСКАЯ ХАРАКТЕРИСТИКА ЛИЧНОСТИ ПРЕСТУПНИКА, ПОСЯГАЮЩЕГО НА ЖИЗНЬ НОВОРОЖДЕННОГО РЕБЕНКА

Исследуются возможности предупреждения посягательств на жизнь новорожденных детей. Представлена авторская разработка криминологического портрета лица, посягающего на жизнь новорожденного.

Ключевые слова: посягательства на жизнь новорожденных детей, криминологическая характеристика личности преступника, женщины как преступника.

Сегодня понимание механизмов противоправного поведения требует углубленного изучения особенностей совершающих данные деяния лиц, так как личность является не только про-