УДК 343.4

С. Д. Петроченков, *кандидат юридических наук, доцент кафедры оперативно-розыскной деятельности Рязанского филиала Московского университета МВД России имени В. Я. Кикотя*
e-mail: sedm-09-07@yandex.ru

УГОЛОВНАЯ ОТВЕТСТВЕННОСТЬ ЗА НЕЗАКОННЫЙ ОБОРОТ И ИСПОЛЬЗОВАНИЕ СПЕЦИАЛЬНЫХ ТЕХНИЧЕСКИХ СРЕДСТВ, ПРЕДНАЗНАЧЕННЫХ ДЛЯ НЕГЛАСНОГО ПОЛУЧЕНИЯ ИНФОРМАЦИИ, В РОССИЙСКОЙ ФЕДЕРАЦИИ И РЕСПУБЛИКЕ БЕЛАРУСЬ

На основе сравнительного анализа законодательства Российской Федерации и Республики Беларусь, международных документов Союзного государства предлагаются пути дальнейшего совершенствования уголовного закона в части ответственности за незаконный оборот и использование специальных технических средств, предназначенных для негласного получения информации.

Ключевые слова: Уголовный кодекс Российской Федерации, Уголовный кодекс Республики Беларусь, сравнительный анализ, оборот специальных технических средств, предназначенных для негласного получения информации, использование специальных технических средств, предназначенных для негласного получения информации, совершенствование законодательства.

S. D. Petrochenkov, *Candidate of Juridical Sciences, Associate Professor of the Department of Detective Activity of the Ryazan Branch of Moscow University of the MIA of the Russia named after V. Y. Kikot*
e-mail: sedm-09-07@yandex.ru

CRIMINAL LIABILITY FOR ILLEGAL TRAFFICKING AND USE OF SPECIAL TECHNICAL EQUIPMENT INTENDED FOR SECRET RECEIVING OF INFORMATION IN THE RUSSIAN FEDERATION AND THE REPUBLIC OF BELARUS

Based on a comparative analysis of the legislation of the Russian Federation and the Republic of Belarus, international documents of the Union State, ways are proposed to further improve the criminal law in terms of liability for illegal trafficking and the use of special technical equipment intended for secret receiving of information.

Keywords: the Criminal code of the Russian Federation, the Criminal code of the Republic of Belarus, comparative analysis, trafficking of special technical equipment intended for secret receiving of information, using of special technical equipment intended for secret receiving of information, improvement of legislation.

Специальные технические средства (СТС), предназначенные для негласного получения информации, в качестве оперативной техники успешно применяются в раскрытии преступлений как в Российской Федерации, так и в Республике Беларусь. Поскольку СТС могут использоваться для незаконного получения информации лицами, не относящимися к числу сотрудников оперативно-розыскных органов, законодательство обоих государств ограничивает оборот и использование указанных средств. Так, международные акты Евразийского экономического союза (Россия, Беларусь, Казахстан, Армения, Кыргызстан) относят СТС к перечню предметов, ввоз и вывоз которых на территорию и с территории ЕАЭС ограничен [2]. Однако, несмотря на Таможенный союз и строительство Союзного государства, внутреннее законодательство Российской Федерации и Республики Беларусь, ограничивающее оборот и использование СТС, имеет существенные различия.

За незаконный оборот СТС, т. е. за *приобретение*, *производство* или *сбыт* без получения необходимой для этого лицензии (здесь и далее курсив наш. – *С. П.*), ст. 138.1 УК Российской Федерации) предусмотрена ответственность. Уголовный кодекс также запрещает незаконное использование СТС, но лишь в одном случае – при получении сведений, составляющих государственную тайну (п. «г» ч. 2 ст. 283.1 УК РФ). До 2011 г. использование СТС являлось квалифицирующим признаком такого преступления, как нарушение тайны переписки, телефонных переговоров, телеграфных или иных сообщений (ст. 138 УК РФ), однако Федеральным законом от 7 декабря 2011 г. № 420-ФЗ этот признак был исключен из УК РФ и в настоящий момент исполь-

зование СТС сохраняет свое уголовно-правовое значение только в части получения сведений, составляющих государственную тайну. В соответствии с расположением обозначенных статей в составе УК РФ их объектами являются общественные отношения, связанные с защитой личных прав и свобод человека и гражданина (ст. 138.1 УК РФ), а также информационной безопасности государства (ст. 283.1 УК РФ) [5].

В свою очередь, исследование уголовного законодательства Республики Беларусь позволяет выделить два основных объекта преступных посягательств, связанных с незаконным оборотом и использованием СТС: установленный порядок управления (ст. 375^1, 376 УК Республики Беларусь); конституционные права и свободы человека и гражданина (ст. 203 УК Республики Беларусь) [3].

Незаконный оборот СТС, в качестве которого рассматриваются *изготовление* или *приобретение в целях сбыта* либо *сбыт* (ст. 376 УК Республики Беларусь), по мнению белорусского законодателя, посягает на установленный порядок управления. Ответственность за незаконное использование СТС предусмотрена в качестве квалифицирующего признака преступления при умышленном незаконном нарушении тайны переписки, телефонных или иных переговоров, почтовых, телеграфных или иных сообщений граждан (ч. 2 ст. 203 УК Республики Беларусь – аналог ранее действовавшей редакции ч. 2 ст. 138 УК РФ), а также при незаконном собирании либо получении сведений, составляющих государственные секреты (ч. 2 ст. 375^1 УК Республики Беларусь). Ранее УК Республики Беларусь также предусматривал уголовную ответственность за совершенные с использованием СТС незаконное собирание либо распространение сведений о частной жизни, составляющих личную или семейную тайну другого лица, без его согласия (ч. 2 ст. 179 УК Республики Беларусь), однако в последующем эта статья из кодекса была исключена.

Таким образом, в белорусском законодательстве незаконное использование СТС является квалифицирующим признаком преступлений, ответственность за которые предусмотрена ст. 275^1, 203 УК Республики Беларусь, однако на другие составы преступлений этот признак не распространяется. Тем самым в Республике Беларусь, как и в Российской Федерации, использование СТС криминализировано лишь для отдельных случаев.

Отличительной особенностью белорусского законодательства является содержание в составе УК Республики Беларусь ст. 354, криминализирующей разработку, использование, распространение либо сбыт вредоносных компьютерных программ или специальных программных (аппаратных) средств. По своему содержанию она объединяет нормы ранее действовавшей редакции этой же статьи, криминализировавшей разработку, использование, распространение либо сбыт вредоносных программ, и исключенной ст. 353 УК Республики Беларусь. Последняя содержала запрет на *изготовление с целью сбыта* либо *сбыт специальных программных или аппаратных средств* для получения неправомерного доступа к защищенной компьютерной системе или сети. Введением в уголовное законодательство ст. 354 разрешило проблему квалификации действий, связанных с созданием или использованием программного обеспечения, заведомо разработанного для неправомерного получения компьютерной информации.

Исследование уголовного законодательства зарубежных государств позволило найти и другой способ решения этого вопроса: в уголовном кодексе закрепляются две отдельные статьи, одна из которых устанавливает ответственность за незаконный оборот специальных программных средств для негласного получения компьютерной информации, другая – за оборот вредоносных компьютерных программ. Главным критерием разграничения этих преступлений является предназначение программного обеспечения: в первом случае – неправомерный доступ к компьютерной информации, а во втором – несанкционированное уничтожение, блокирование, модификация или копирование компьютерной информации [4, 6]. Этот же способ законодательного решения был предусмотрен ранее действовавшими редакциями ст. 353, 354 УК Республики Беларусь.

Согласно действующей редакции УК Республики Беларусь ст. 354 является специальной по отношению к ст. 376, ограничивающей незаконный оборот СТС, и подлежит применению в случае незаконной разработки, использования, распространения или сбыта компьютерных программ, заведомо предназначенных для неправомерного завладения компьютерной информацией либо нарушения работы компьютерной системы, сети или машинного носителя. Тем самым дифференциация уголовной ответственности призвана внести ясность в конкуренцию право-

вых норм, предусмотренных ст. 354 и 376 УК Республики Беларусь. В современных условиях всеобщей информатизации такая мера вполне оправданна.

Сравнительный анализ российского и белорусского уголовного законодательства позволяет сделать общие выводы.

Указанный в уголовных законах обоих государств перечень действий, составляющих незаконный оборот СТС, является неполным. Несмотря на установленное требование лицензирования для ввоза и вывоза СТС через границу Таможенного союза, эти действия не являются уголовно наказуемыми ни в Российской Федерации, ни в Республике Беларусь. Ввиду того, что значительная часть запрещенных к обороту СТС поступает на территорию Союзного государства через таможенную границу с территории Китайской Народной Республики, закрепление уголовной (а не административной) ответственности за незаконный ввоз и вывоз СТС могло бы способствовать сокращению их оборота и использования. Другим позитивным нововведением для законодательства обоих государств могла бы стать криминализация незаконной разработки СТС, что также имело бы превентивное значение. В Российской Федерации такая мера, помимо прочего, может способствовать приведению бланкетной нормы ст. 138.1 УК РФ в соответствие со ст. 12 Федерального закона от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности», включающей в перечень видов деятельности, на осуществление которых требуется получение лицензии, *разработку*, *производство*, *реализацию* и *приобретение в целях продажи СТС* [1].

По этой причине необходимо расширить и скорректировать перечень действий, криминализированных ст. 138.1 УК РФ. К незаконному обороту СТС следует относить незаконные разработку, производство, реализацию, приобретение в целях продажи, ввоз на территорию Российской Федерации и вывоз данных средств за ее пределы. Белорусское уголовное законодательство, очевидно, также нуждается в расширении перечня действий, составляющих незаконный оборот СТС, по крайней мере, в части установления ответственности за их ввоз и вывоз через таможенную границу Союзного государства.

С учетом того что незаконный оборот СТС напрямую не посягает на неприкосновенность конституционных прав граждан, а лишь создает возможность такого посягательства, правильнее считать объектом незаконного оборота СТС установленный порядок управления. В данном аспекте позиция белорусского законодателя представляется более логичной, и с этой точки зрения включение состава преступления, предусмотренного ст. 138.1 УК РФ, в гл. 32 «Преступления против порядка управления», являлось бы рациональной мерой. Однако с учетом сложившейся практики такое перемещение статьи может усложнить и без того запутанную правоприменительную ситуацию и едва ли целесообразно.

Что касается криминализации незаконного использования СТС в качестве квалифицирующего признака преступления, то целесообразность такой меры сомнительна. В настоящее время преступления, связанные с посягательством на охраняемую законом тайну, все чаще совершаются с применением таких технических средств, как аппаратура негласной аудиовидеозаписи (диктофоны, фото-, видеокамеры и др.), устройства слежения за перемещениями объектов (трекеры навигационных систем, мобильные устройства), устройства вскрытия автомобильной сигнализации (кодграбберы), устройства считывания данных банковских платежных карточек (скиммеры).

В этих случаях совершенные деяния должны дополнительно квалифицироваться по статье, предусматривающей ответственность за незаконный оборот СТС. С учетом многообразия преступлений в сфере защиты тайны указывать в каждом случае (или применительно к отдельным преступлениям) квалифицирующий признак использования СТС едва ли целесообразно.

В этой связи рациональной мерой следовало бы считать декриминализацию противоправных деяний, предусматривающих использование СТС в качестве квалифицирующего признака преступления.

В российском уголовном законе имеется существенный пробел: программное обеспечение, предназначенное для негласного получения информации, не относится к числу вредоносных программ, указанных в ст. 273 УК РФ. Оно законодательно отнесено к СТС, однако применение ст. 138.1 УК РФ в случае его использования затруднительно, так как для оборота компьютерных

программ почти не свойственны действия, совершаемые СТС: производство, ввоз и вывоз через таможенную границу.

Считаем, что существующий пробел необходимо восполнить, включив в состав УК РФ статью, криминализирующую оборот программного обеспечения, предназначенного для негласного доступа к компьютерной информации. Отнесение таких средств к числу вредоносных программ считаем нецелесообразным ввиду направленности их на негласное получение информации (а не на несанкционированное уничтожение, блокирование, модификацию, копирование компьютерной информации или нейтрализацию средств ее защиты). Кроме того, программное обеспечение, предназначенное для негласного получения информации, в перечне, утвержденном Правительством Российской Федерации, отнесено к числу СТС. Отнесение их к числу вредоносных программ способно породить коллизии в отечественном законодательстве.

Совокупность полученных в результате сравнительного исследования выводов позволяет предложить меры, которые способны положительно повлиять на решение существующих проблем в правоприменительной деятельности обоих государств и могут быть реализованы в рамках единой уголовной политики Союзного государства.

Список использованных источников

1. О лицензировании отдельных видов деятельности [Электронный ресурс] : Федер. закон, 4 мая 2011 г., № 99-ФЗ : в ред. Федер. закона от 02.07.2021 г. // КонсультантПлюс. Россия / ЗАО «КонсультантПлюс». – М., 2021.

2. Положение о ввозе на таможенную территорию Евразийского экономического союза и вывозе с таможенной территории Евразийского экономического союза специальных технических средств, предназначенных для негласного получения информации [Электронный ресурс] : утв. решением Коллегии Евразийской экономической комиссии, 21 апр. 2015 г., № 30 // КонсультантПлюс. Россия / ЗАО «КонсультантПлюс». – М., 2021.

3. Уголовный кодекс Республики Беларусь [Электронный ресурс] : 9 июля 1999 г., № 275-З : принят Палатой представителей 2 июня 1999 г. : одобр. Советом Респ. 24 июня 1999 г. : в ред. Закона Респ. Беларусь от 26.05.2021 г. / Нац. центр правовой информ. Респ. Беларусь. – Режим доступа: http://pravo.by. – Дата доступа: 05.10.2021.

4. Уголовный кодекс Республики Узбекистан [Электронный ресурс] : 22 сентября 1994 г., № 2012-XII. – Режим доступа: http://lex.uz/oloes/111457. – Дата доступа: 05.10.2021.

5. Уголовный кодекс Российской Федерации [Электронный ресурс] : 13 июня 1996 г., № 63-ФЗ : принят Гос. Думой 24 мая 1996 г. : одобр. Советом Федерации 5 июня 1996 г. : в ред. Федер. закона от 01.07.2021 г. // КонсультантПлюс. Россия / ЗАО «КонсультантПлюс». – М., 2021.

6. Уголовный кодекс Франции [Электронный ресурс] : 22.07.1992 г. – Режим доступа: http://constitutions.ru/?p=25017. – Дата доступа: 05.10.2021.

Дата поступления в редакцию: 04.10.2021

УДК 343.24

***Е. А. Реутская**, кандидат юридических наук, старший преподаватель кафедры уголовного права и криминологии Академии МВД Республики Беларусь*
e-mail: ellen-britova@rambler.ru

ЭВОЛЮЦИЯ ИНСТИТУТА НАКАЗАНИЯ В УГОЛОВНОМ ПРАВЕ

На основе анализа существующих в юридической литературе подходов обосновывается необходимость оптимизации системы уголовных наказаний. Особо обращается внимание на обусловленность содержания санкций статей Особенной части уголовного закона видами наказания. Изучение основополагающих идей школ уголовного права позволило предположить, что существующая система наказаний является избыточной, а реальная оценка тяжести карательного воздействия некоторых видов наказания изменилась с течением времени.

Ключевые слова: наказание, система наказаний, школы уголовного права, санкция статьи Особенной части.