ние водителем транспортного средства требования о прохождении медицинского освидетельствования…) законодатель указал на уголовную преюдицию в виде судимости за совершение преступлений, предусмотренных ч. ч. 2, 4, 6 ст. 264 либо ст. 264.1 УК РФ, таким образом, отнеся административную преюдицию к общественно опасному деянию.

В-третьих, законодатель нарушает принцип равенства граждан перед законом, когда при повторном совершении правонарушения (ч. 3.1 ст. 12.16, ч. 5 ст. 12.15, ч. 3 ст. 12.12, ч. 3 ст. 12.10, ч. 6, 7 ст. 12.9 КоАП РФ) в одних случаях усиливается лишь административное наказание, в другом (ст. 264.1 УК РФ) – возникает основание для привлечения к уголовной ответственности.

В-четвертых, законодателем использован институт административно-правового рецидива правонарушений, когда степень опасности административного правонарушения при неоднократном (повторном) его совершении приобретает уровень общественной опасности преступления.

На наш взгляд, повторное совершение одного и того же административного деяния образует общественную опасность и как следствие – нуждается в криминализации.

Таким образом, целесообразно действующую редакцию ст. 264.1 УК РФ изменить следующим образом:

часть 1: «Управление транспортным средством лицом, находящимся в состоянии опьянения, подвергнутым административному наказанию за аналогичное правонарушение в течение года или за невыполнение водителем транспортного средства законного требования уполномоченного должностного лица о прохождении медицинского освидетельствования на состояние опьянения»;

часть 2: «Управление транспортным средством лицом, находящимся в состоянии опьянения и имеющим судимость за совершение преступления, предусмотренного частями второй, четвертой или шестой статьи 264 настоящего Кодекса либо настоящей статьей».

Считаем, что предлагаемые изменения и дополнения в ст. 264.1 УК РФ будут способствовать эффективной унификации уголовно-правовой нормы, совершенствованию правоприменительной практики и реализации общей и частной превенции.

[1] О внесении изменений в отдельные законодательные акты Российской Федерации по вопросу усиления ответственности за совершение правонарушений в сфере безопасности дорожного движения : Федеральный закон от 31.12.2014 № 528-ФЗ // Российская газета. 2015. № 1.

[2] Официальный сайт Судебного департамента при Верховном Суде Российской Федерации. URL: http://www.cdep.ru/index.php?id=79&item=3212.

[3] Статистические данные получены с автоматизированной информационно-статистической системы (АИСС) «Статистика-Регион» в ГУ МВД России по Красноярскому краю.

Тирранен В.А.,

кандидат юридических наук
Красноярский государственный
аграрный университет

АКТУАЛЬНЫЕ ПРОБЛЕМЫ УГОЛОВНОГО ПРАВА В СФЕРЕ БОРЬБЫ С КИБЕРПРЕСТУПНОСТЬЮ

Важным элементом жизни современного общества и государства стало развитие информационных технологий, которые плотно внедряются в современную жизнь. Граница между государствами в информационном поле исчезает, обмен информацией становится мгновенным. Ключевой угрозой в таких реалиях становятся не отдельные преступники, совершающие преступления с высоким уровнем общественной опасности, а организованные преступные группы, в том числе преступные сообщества, связанные с организацией киберпреступлений. В настоящее время деятельность правоохранительных органов России не в полной мере соответствует реальным угрозам киберпреступности в стране и в мире. Уголовное законодательство России не унифицировано с международны-

ми нормами и законодательством зарубежных стран, что препятствует интеграции России в международный процесс борьбы с киберпреступностью. Для предотвращения распространения киберпреступлений необходимо решить проблему интеграции международных норм по идентификации киберпреступлений и борьбе с киберпреступностью в национальное законодательство России.

Определение «киберпреступности» и «киберпреступления» отсутствует в официальных документах, переведенных на русский язык. Не раскрывается оно и в Конвенции Совета Европы о компьютерных преступлениях (Convention on Cybercrime ETS № 185, Будапешт, 23.11.2001[1]), но это не мешает многим зарубежным авторам давать определения данному термину. Например, достаточно широко используется определение, сформулированное Д. Халдером (Debarati Halder) и К. Джаишанкаром (Karuppannan Jaishankar), согласно которому киберпреступления – это преступления, которые совершаются в отношении отдельного лица или группы лиц, с криминальным мотивом, с умыслом на нанесение ущерба репутации жертвы, причинение физического или морального ущерба, либо материального вреда потерпевшему как прямо, так и косвенно, с использованием телекоммуникационных сетей, таких как Интернет (чаты, электронные письма, рекламные баннеры и публичные группы) и мобильные телефоны (SMS / MMS, мессенджеры)[2].

В настоящее время организованная преступность открыла для себя новые возможности преступной деятельности и новые способы совершения хорошо известных преступлений. При этом во всем мире количество совершаемых киберпреступлений растет год от года. По данным Norton Cybercrime Report[3], еще в 2012 г. ущерб от совершения таких преступлений только в России оценивался в 2 миллиарда долларов США в год, а во всем мире – более 110 миллиардов долларов США. К 2015 г. суммарный ущерб от киберпреступлений вырос до 388 миллиардов долларов США. За 2012 г. в России, по данным Norton Cybercrime Report, были выявлены более 30 миллионов деяний, имеющих признаки киберпреступлений. В то же время, по официальным данным МВД России, за этот период количество зарегистрированных преступлений в сфере компьютерной информации в России не превысило 2820.

Высокая латентность киберпреступлений обусловлена во многом тем, что потерпевшие не только не осознают противоправности совершаемого в отношении них посягательства, но и зачастую не замечают его признаков и следов. Так, гражданин, не имеющий специальных навыков и образования, не может логически связать электронное письмо от неизвестного отправителя, которое при попытке прочтения скрытно устанавливает вредоносное программное обеспечение, и списание злоумышленником с банковской карты гражданина денежных средств.

Развитию организованной киберпреступности также способствует высокая доля анонимности пользователей большинства информационно-телекоммуникационных сетей, использующих различного рода программные средства обеспечения персональной анонимности. Широко распространенная анонимная сеть Tor примечательна использованием оригинального метода обеспечения анонимности передаваемых сигналов: сообщения в ней неоднократно шифруются и отсылаются единым пакетом через несколько сетевых узлов, называемых «луковыми» маршрутизаторами. Каждый такой маршрутизатор удаляет «слой» шифрования, чтобы открыть трассировочные инструкции и отослать сообщения на следующий маршрутизатор, где все повторяется. Из-за этого промежуточные узлы не знают источник, пункт назначения и содержание сообщения, а итоговый узел не знает ничего, кроме условного «имени» адресанта. В настоящее время технология «луковой» маршрутизации, используемой в Tor, считается устаревшей, уступая пространство I2P (invisible internet project – проект «невидимый интернет»), оверлейной сети, устойчивой к отключению первичных узлов и использующей многослойное («чесночное») шифрование,

включающее в себя туннелирование и шифрование транспортного уровня, что устраняет уязвимость к анализу синхронизации – основному способу принудительной деанонимизации пользователей Tor.

С использованием анонимных сетей совершаются значительное количество преступлений, связанных с незаконным оборотом наркотиков, оружия, запрещенной информации. Выявление и раскрытие таких деяний осложняется тем, что понимание сущности многих киберпреступлений у правоприменителя отсутствует, а потому в различных регионах России практика привлечения к уголовной ответственности за аналогичные деяния существенно разнится. В большей мере это явление связано с несовершенством законодательства, описывающего признаки киберпреступлений крайне неоднозначно, в то время как постоянная эволюция возможностей для совершения преступлений создает новые угрозы для пользователей глобальных информационно-телекоммуникационных сетей.

В настоящее время российское уголовное законодательство далеко от адаптации к нормам международного регулирования в сфере киберпреступности. Не подписанная Россией Конвенция Совета Европы о киберпреступности подразделяет преступления в киберпространстве на несколько групп, включая преступления против конфиденциальности и доступности компьютерных данных и систем; незаконное использование компьютерных средств и технологий; производство и предоставления детской порнографии; нарушения в сфере авторского права; распространение информации дискриминационного характера, подстрекающей к насильственным действиям, разжиганию ненависти или вражды. Несмотря на то, что многих из этих преступлений предусмотрены в УК РФ, они не отражают специфику киберпреступлений, требующих специального подхода к предупреждению, выявлению и расследованию.

Только в 2011 г. УК РФ перестал использовать термин «ЭВМ», но оперативно изменяющиеся реалии киберпреступности до сих пор в нем не отражены. Основной проблемой является отсутствие понимания необходимости глобальной борьбы с киберпреступностью, особенно организованной, поскольку борьба с ней в рамках отдельно взятого государства способна дать заметные результаты только при условии полного физического исключения информационно-телекоммуникационных сетей этого государства из глобальной сети Интернет и сетей телефонной связи, что обернется невозможностью быстрого обмена информацией и поспособствует стагнации в экономике и науке. Таким образом, для эффективной борьбы с такой преступностью первым этапом должна стать унификация уголовного законодательства различных стран в сфере борьбы с киберпреступлениями, по аналогии с унификацией законодательства в сфере преступлений против мира и безопасности человечества. Закрепление термина «киберпреступление» в уголовном праве России поспособствует единообразию в подходе к определению таких преступлений.

Предпринятая уже попытка отечественного законодателя скопировать сложившиеся правила регулирования вредоносных программ с зарубежного термина «malware» (malicious software (англ.) – буквально «вредоносное программное обеспечение»[4]) остановилась на полпути: зарубежные законодатели помимо общего «вредоносного программного обеспечения», выделяют и так называемое «нежелательное программное обеспечение», к которому относятся, например, программы класса «adware» (программное обеспечение, навязчиво показывающее рекламу), относимые УК РФ к вредоносным по признаку несанкционированной модификации компьютерной информации, однако не всегда объективно обладающие достаточной степенью общественной опасности для криминализации их создания и использования. Для очевидно преступных программ зарубежные специалисты и правоприменители ряда стран используют термин «crimeware» (criminal software (англ.) – буквально «преступное программное обеспечение»[5]), т.е. про-

граммное обеспечение, используемое именно для получения доступа к защищенным сетям, корпоративным и государственным тайнам, автоматизированного хищения информации о платежных реквизитах пользователей, либо списания финансовых средств с электронных платежных систем и пластиковых карт. При этом область регулирования имеет устоявшуюся и постоянно используемую терминологию, неприменимую и невоспроизводимую в уголовном законе (вирусы, руткиты, трояны, эксплойты). В то же время это не означает невозможности однозначного отделения «преступного» программного обеспечения от просто «вредоносного», но требует детального закрепления данных терминов и их признаков в специализированных нормативно-правовых актах.

В результате проведенного анализа актуальных проблем уголовного права в сфере борьбы с киберпреступностью можно выявить некоторую бессистемность изменений, вносимых в уголовный закон, в то время как нормы, касающиеся киберпреступности, со всей очевидностью участвуют в обеспечении противодействия международной организованной киберпреступности и, исходя из этого, не должны противоречить как международно-правовым нормам, так и отраслям национального права зарубежных стран. Отсутствие системного подхода к развитию уголовного законодательства неоднократно подвергалось критике.

В настоящее время ключевой задачей уголовного права России в сфере борьбы с киберпреступностью является интеграция международного законодательства в сфере борьбы с киберпреступностью в систему уголовного права России, а также выработка единого подхода к определению признаков киберпреступности в России. Преступления такого рода не имеют границ, и могут совершаться против интересов России лицом, находящимся за ее пределами, что определяет специфику киберпреступлений.

[1] Конвенция Совета Европы о компьютерных преступлениях. Будапешт, 23/11/2001. ETS № 185. URL: http://www.coe.int/ru/web/conventions/full-list/-/conventions/treaty/185 (дата обращения: 25.09.2016).

[2] Halder D., Jaishankar K. Cybercrime and the Victimization of Women: Laws, Rights, and Regulations. Hershey, PA, USA: IGI Global. 2011. 280 p.

[3] Norton Cybercrime Report. URL: http://us.norton.com/cybercrimereport (дата обращения: 25.09.2016).

[4] Software Terms : Malware Definition. URL: http://techterms.com/definition/malware (дата обращения: 01.03.2016).

[5] Jakobsson M., Ramzan Z. Crimeware: Understanding New Attacks and Defenses. USA: Addison-Wesley Professional. 2008. 608 p.

Астахова А.О.

Сибирский юридический институт
МВД России (г. Красноярск)

СОВЕРШЕНСТВОВАНИЕ ЗАКОНОДАТЕЛЬНОГО ЗАКРЕПЛЕНИЯ УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ ЗА УКЛОНЕНИЕ ОТ АДМИНИСТРАТИВНОГО НАДЗОРА

В современном обществе не снижается актуальность вопроса профилактики преступлений. Особенное внимание в этом плане уделяется мерам, направленным на предотвращение совершения преступлений лицами, ранее судимыми, отбывшими наказание в виде лишения свободы и освободившимися из мест лишения свободы по отбытии наказания.

Принятие Федерального закона от 6 апреля 2011 г. № 64-ФЗ «Об административном надзоре за лицами, освободившимися из мест лишения свободы» (далее – Закон об административном надзоре) обусловило введение в УК РФ ст. 314.1 «Уклонение от административного надзора», которая закрепила уголовную ответственность лиц, в отношении которых установлен административный надзор при освобождении из мест лишения свободы, за неприбытие без уважительных причин к избранному месту жительства или пребывания в определенный срок, а равно самовольное