УДК 343.92

Асрян Армен Лаврентьевич,
Донецкий национальный университет,
г. Донецк, Донецкая Народная Республика
armen.asryan.00@mail.ru

Современные проблемы осуществления оперативно-розыскной деятельности в сфере борьбы с киберпреступностью

В статье рассматриваются правовые проблемы, связанные с необходимостью осуществления оперативно-розыскной деятельности в киберпространстве, а также затрагиваются проблемные вопросы недостаточной проработанности отечественной правовой системы, ее норм и принципов, касающихся основных аспектов противодействия киберпреступности. Основываясь на результатах анализа доктринальных положений теории оперативно-розыскной деятельности, действующего законодательства и правоприменительной практики в области выявления, предупреждения, пресечения и раскрытия киберпреступлений, раскрываются основные понятия по теме преступности в виртуальном пространстве, а также выдвигаются предложения по совершенствованию правового механизма в сфере борьбы с киберпреступностью.

Ключевые слова: *Оперативно-розыскная деятельность, киберпреступность, информационные технологии, виртуальное пространство, сеть, интернет.*

Asryan Armen Lavrent'evich,
Donetsk National University, Faculty of Law,
Donetsk, Donetsk People's Republic
armen.asryan.00@mail.ru

Modern problems of implementation of operative-search activities in the field of fight against cyber crime

The article discusses the legal problems associated with the need to conduct operational-search activities in cyberspace, as well as touches on the problematic issues of the lack of elaboration of the domestic legal system, its norms and principles regarding the main aspects of combating cybercrime. Based on the results of the analysis of the doctrinal provisions of the theory of operative-search activity, current legislation and law enforcement practice in the field of detection, prevention, suppression and disclosure of cybercrimes, the basic concepts on the topic of crime in the virtual space are revealed, as well as proposals are made to improve the legal mechanism in the fight against cybercrime.

Keywords: *operational-search activities, cybercrime, information technology, virtual space, network, Internet.*

Актуальные тенденции развития мировых общественных отношений характеризуются высокой степенью интеграции в социальную действительность новых информационно-коммуникационных технологий. Процесс глобальной оцифровки информации, начавшийся еще во второй половине прошлого столетия, несомненно, является значимым феноменом, регулирование основ которого и по сей день требует особых и специальных знаний в указанной сфере. В связи с этим закономерным является тот факт, что стремительное распространение новых информационных технологий не дает возможности полно, объективно, а главное, своевременно осмысливать криминальные новшества в киберпространстве и сопряженные с ними риски. Таковыми можно считать не только новые компьютерные вирусы, уязвимости и закладки, но и реальную угрозу несанкционированного доступа, отсутствие приватности, утечку персональных данных пользователей сети, тотальный контроль отечественного рынка иностранными производителями и т. п. [6, с. 9].

С целью осуществления более качественной правоохранительной деятельности, защиты конституционных прав человека и гражданина в области информационной безопасности и успешной борьбы с киберпреступностью в Уголовный кодекс Российской Федерации был добавлен ряд составов преступлений, связанных непосредственно с общественно-опасными посягательствами в сфере компьютерной информации, образовавших отдельную главу Уголовного закона, а именно: неправомерный доступ к компьютерной информации; создание, использование и распространение вредоносных компьютерных программ; нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей; неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации [5, ст. 272–274.1]. Однако встречаются также иные уголовно-правовые составы, так или иначе относимые к категории киберпреступлений, например, мошенничество в сфере компьютерной информации [5, ст. 159.6]. Более того, так как под киберпреступлением понимается всякое преступление, совершенное в виртуальном пространстве, то указанным понятием охватываются все противоправные общественно-опасное деяния, совершенные с использованием вычислительных машин или сети Интернет.

Эффективная борьба с преступностью, образуемой в результате совершения теми или иными лицами вышеуказанных преступлений, является одной из приоритетных задач правоохранительных органов. Как по данному поводу указывает А. Л. Осипенко: «Обозначенные обстоятельства, связанные с глубокими изменениями социальной реальности, подтверждают, что борьба с преступностью в киберпространстве уже невозможна без применения оперативно-розыскных сил, средств и методов» [3, с. 39]. Стоит заметить, что современное законодательство об оперативно-розыскной деятельности предусматривает особый вид оперативно-розыскного мероприятия – получение компьютерной

информации, благодаря которому у соответствующих должностных лиц, ведущих правоохранительную деятельность, существует прямая возможность воздействовать на информационную среду с целью выявления, предупреждения, пресечения и раскрытия киберпреступлений, а также выявление и установления лиц, их подготавливающих, совершающих или совершивших [2, ст. 6]. Тем не менее, попытки активного внедрения в правоприменительную практику процесса осуществления оперативно-розыскной деятельности для целей борьбы с преступлениями в сфере информационных технологий небезосновательно будут характеризоваться большими проблемами. Прежде всего, это связано с трансграничным характером киберпреступности. Трансграничное преступление, как правило, характеризуется тем, что лицо, совершившее или совершающее его, находится физически в одном государстве, в то время как предмет преступного посягательства располагается в другом. В ином государстве могут находиться орудия и средства совершения преступления, доступ к которым преступник осуществляет дистанционно. При раскрытии трансграничных преступлений нередко складываются ситуации столкновения различных интересов и правовых систем, связанные с невозможностью точно определить, в чьем ведении находится защищаемый информационный ресурс или информационное общественное отношение [3, с. 42]. Указанная особенность, к слову, практически полностью исключает возможность каким-либо образом достичь задач оперативно-розыскной деятельности, не говоря уже о том, что это является значительным пробелом в законодательстве всех без исключения государств. По данному поводу необходимо подчеркнуть, что разрешение соответствующей проблемы возможно лишь при усилении международного сотрудничества между всеми государствами международного сообщества, т. к. именно благодаря синхронизации национальных законодательств различных стран мира по вопросу борьбы с киберпреступностью возможно установить более четкие правовые рамки и направления для установления, преследования и привлечения к ответственности лиц, нарушающих правила киберпезопасности населения того или иного государства [4, с. 95].

Не менее важной проблемой на пути к установлению успешной практики пресечения и предупреждения киберпреступлений является низкий уровень осведомленности сотрудников правоохранительных органов о компьютерных технологиях, характере взаимоотношений субъектов в виртуальном пространстве, целях и мотивах киберпреступников и других факторах и обстоятельствах, непосредственно служащих основой для совершения того или иного противоправного и общественно-опасного посягательства, сопряженного с использованием информационно-коммуникационных технологий и средств. Разрешение отмеченной проблемы видится, в первую очередь, в изменении основополагающих подходов к обучению в отечественной образовательной системе и в ходе профессиональной деятельности соответствующих кадров правоохранительных органов. Как отмечает М. В. Дульцев: «Правоохранительные органы должны создать действенную политику безопасности в области информационных технологий и должны готовить персонал таким образом, чтобы развивать культуру осведомленности сотрудников полиции в области кибербезопасно-

сти» [1, с. 49]. Так, целесообразно образовать в рамках оперативно-розыскной науки отдельное теоретическое направление об особенностях виртуального пространства как среды осуществления оперативно-розыскной деятельности, а также внедрить в образовательную программу по юридическим специальностям тех учебных дисциплин, которые бы не только давали возможность будущим работникам правоохранительной системы государства вести поиск, сбор и систематизацию информации с использованием сети Интернет, а и позволяли бы обучающимся получать информацию об основных понятиях, категориях, процессах во Всемирной сети, а также методах и средствах выявления в ней криминогенных ситуаций. В свою очередь, реформирование организации работы и должный уровень профессионального просвещения по указанному направлению в структурных подразделениях правоохранительных органов также необходимо привести в соответствие с современными требованиями и вызовами социальной действительности посредством контроля при приеме на должность, требующую специальных знаний и в ходе осуществления сотрудником своих должностных полномочий.

Учитывая важность и обоснованную необходимость осуществления оперативно-розыскной деятельности в борьбе с киберпреступностью, следует также отметить, что совершенствование указанного механизма является одним из главных условий установления правопорядка в киберпространстве по той причине, что именно выявление, своевременное предупреждение и пресечение киберпреступлений позволяют сохранить в целостности те общественные отношения, которые с недавних пор находятся под особой охраной уголовно-правового законодательства.

Библиографический список

1. Дульцев М. В., Нурлыбаева Г. К. Сотрудничество в сфере борьбы с киберугрозами. М. : Академия управления МВД России, 2016. С. 43–49.

2. Закон Российская Федерация от 12.08.1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» (с учетом изменений и дополнений) // Собрание законодательства Российской Федерации. 1995. № 33. Ст. 3349.

3. Осипенко А. Л. Оперативно-розыскная деятельность в киберпространстве: ответы на новые вызовы // Научный вестник Омской академии МВД России 2010. № 2 (37). С. 38–43.

4. Тропина Т. Л. Борьба с киберпреступностью: возможна ли разработка универсального механизма? М. : Институт права и публичной политики, 2012. № 3(4). С. 86–95.

5. Уголовный кодекс Российской Федерации от 13.06.1996 г. № 63-ФЗ (ред. от 04.11.2019) // Собрание законодательства Российской Федерации. 1996. № 25. Ст. 2954.

6. Шаталов А. С. Разработка методических основ расследования преступлений, совершаемых с помощью компьютерных и сетевых технологий: проблемы, перспективы, тенденции // Вестник Сибирского юридического института МВД России. 2018. № 3(32). С. 7–15.