Секция «Уголовный процесс»

Проблемные аспекты осуществления оперативно-розыскной деятельности в сфере борьбы с киберпреступностью

Научный руководитель – Манивлец Элина Евгеньевна

Асрян Армен Лаврентъевич
Студент (бакалавр)
Донецкий национальный университет, Юридический факультет, Кафедра конституционного, международного и криминального права, Донецк, Украина
E-mail: armen.asryan.00@mail.ru

Современные тенденции развития общественных отношений характеризуются высокой степенью интеграции в социальную действительность новых информационно-коммуникационных технологий. Процесс всеобщей 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.

Эффективная борьба с преступностью, образуемой в результате совершения преступлений в сфере компьютерной информации, а также иных общественно-опасных посягательств, совершенных с использованием вычислительной техники и/или сети Интернет, является одной из приоритетных задач правоохранительных органов. По мнению А.Л. Осипенко, обстоятельства, связанные с увеличением криминальной активности в виртуальной реальности, подтверждают, что борьба с преступностью в киберпространстве уже невозможна без применения оперативно-розыскных сил, средств и методов [2].

Необходимо отметить, что современное законодательство об оперативно-розыскной деятельности (далее - ОРД) предусматривает особый вид оперативно-розыскного мероприятия - получение компьютерной информации, благодаря которому у компетентных должностных лиц появляется прямая возможность воздействовать на информационную среду с целью выявления, предупреждения, пресечения и раскрытия киберпреступлений [4]. Тем не менее, попытки активного внедрения в правоприменительную практику процесса осуществления ОРД 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 общественно-опасного посягательства располагается в другом. На территории другого государства могут находиться также орудия и средства совершения соответствующего деяния, доступ к которым преступник осуществляет дистанционно. Процесс раскрытия трансграничных преступлений нередко сопровождается коллизиями политических интересов и правовых систем, связанными с невозможностью точно определить, в чьем ведении находится защищаемый информационный ресурс или информационное общественное отношение [2]. Указанная особенность, к слову, практически полностью исключает возможность каким-либо образом достичь задач ОРД, не говоря уже о том, что это является значительным пробелом в законодательстве всех без исключения государств. Преодоление соответствующей проблемы видится лишь в укреплении международного сотрудничества, т. к. исключительно посредством синхронизации национальных законодательств различных государств по

вопросам борьбы с киберпреступностью могут быть определены более четкие правовые рамки и направления по установлению, преследованию и привлечению к ответственности лиц, нарушающих правила киберпезопасности населения того или иного государства [3].

Не менее важной проблемой на пути к формированию 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, не менее важных факторах и обстоятельствах, непосредственно служащих основой совершения того или иного противоправного и общественно-опасного посягательства в сети Интернет и/или с использованием инновационных информационно-коммуникационных технологий и средств. Разрешение отмеченной проблемы усматривается, в первую очередь, в изменении основополагающих подходов к обучению и подготовке в отечественной образовательной системе и в ходе профессиональной деятельности соответствующих кадров правоохранительных органов.

Как указывают М.В. Дульцев и Г.К. Нурлыбаева, правоохранительным органам следует создать действенную политику безопасности в области информационных технологий и осуществлять подготовку персонала таким образом, чтобы развивать культуру осведомленности сотрудников полиции в области кибербезопасности [1]. Так, целесообразно образовать в рамках оперативно-розыскной науки отдельное теоретическое направление об особенностях виртуального пространства как среды осуществления ОРД, 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.

Источники и литература

1) Дульцев М.В., Нурлыбаева Г.К. Сотрудничество в сфере борьбы с киберугрозами // Российский и международный опыт борьбы с киберпреступностью (на примере Российской Федерации, Германии и США). М., 2016. С. 43–49.

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

3) Тропина, Т.Л. Борьба с киберпреступностью: возможна ли разработка универсального механизма? // Международное правосудие. М., 2012. № 3 (4). С. 86–95.

4) Федеральный закон РФ «Об оперативно-розыскной деятельности» от 12.08.1995 № 144-ФЗ [Электронный ресурс] // СПС КонсультантПлюс. — Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_7519/ (дата обращения: 16.02.2020).