ЗАДАЧИ И ФУНКЦИИ СУБЪЕКТОВ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ В УКРАИНЕ

Вячеслав МАРКОВ,
кандидат юридических наук, старший научный сотрудник,
начальник факультета подготовки специалистов
для подразделений борьбы с киберпреступностью и торговлей людьми
Харьковского национального университета внутренних дел

Summary

The article deals with theoretical research of tasks and functions that should be fulfilled by cybercrime combating units of Ukraine. The author analyzes rules and regulations that at present exist in the field of combating cybercrime in Ukraine. The necessity of more intensive international cooperation in combating cybercrime is emphasized as well as the necessity of the development of regulations that would regulate actions of cybercrime combating units in cyberspace. The role of a cybercrime combating unit in the development of the national system of cyber security is analyzed. The author suggests that the powers of cybercrime combating units should be enlarged authorizing them to launch technical investigative operations when necessary.

Key words: combating cybercrime, law enforcement authorities, tasks, functions, jurisdiction.

Аннотация

В статье проводится теоретическое исследование задач и функций, которые должны решать подразделения борьбы с киберпреступностью в Украине. Проанализирована нормативно-правовая база борьбы с киберпреступностью в Украине. Акцентируется внимание на необходимости углубления международного сотрудничества в борьбе с киберпреступностью, а также разработки соответствующего подзаконного акта, который регламентировал бы деятельность подразделений борьбы с киберпреступностью в киберпространстве. Исследуется роль подразделений борьбы с киберпреступностью в построении национальной системы кибербезопасности. Предлагается расширить полномочия подразделений по борьбе с киберпреступностью, в определенных случаях разрешив им проведение оперативно-технических мероприятий.

Ключевые слова: борьба с киберпреступностью, правоохранительные органы, задачи, функции, компетенция.

Постановка проблемы. Несомненным лидером по интеллектуальной составляющей исполнения преступного замысла на сегодняшний день является киберпреступность. Данный вид преступлений требует определенного массива знаний и навыков в сфере компьютерных технологий со стороны преступников. Очевидно, что противодействовать таким правонарушителям должны правоохранители, обладающие, по крайней мере, не меньшей квалификацией. Огромную роль при этом играет нормативно-правовая и организационная составляющие деятельности последних.

Актуальность темы. Статистика борьбы с киберпреступностью в Украине в настоящее время комплексно не ведется. Вместе с тем следует отметить, что в период с 2002 по 2012 гг. ежегодно регистрировалась незначительная часть преступлений в сфере использования ЭВМ (компьютеров), систем и компьютерных сетей. Максимальный пик пришелся на 2009 г. и составил 217 зарегистрированных преступлений. Указанные данные, по нашему мнению, свидетельствует о высокой латентности такой преступности. Несколько изменилась ситуация в результате реформирования системы уголовного процессуального законодательства 2012 г. В результате в 2013–2014 гг. таких преступлений в совокупности было зарегистрировано больше тысячи. Приведенные цифры свидетельствуют о тенденции роста высокотехнологических преступлений, а также о необходимости активизации усилий правоохранительных органов по противодействию данному негативному явлению.

Вопросы борьбы с киберпреступностью исследовали такие украинские ученые, как А.М. Бандурка, Л.В. Бо-

рисова, И.А. Воронов, В.А. Голубев, В.П. Захаров, М.Ю. Литвинов, А.В. Манжай, Ю.Ю. Орлов, Э.В. Рыжков, Л.П. Скалозуб, Н.Н. Перепелица, Ю.В. Степанов, В.П. Шеломенцев, А.А. Юхно и многие другие авторы. Тем не менее на сегодняшний день остаются нерешенными ряд вопросов в сфере борьбы с киберпреступностью, в частности о необходимой и достаточной компетенции подразделений борьбы с киберпреступностью, которая позволила бы им эффективно выполнять поставленные задачи.

Целью статьи является определение круга задач и функций, которые должны решать подразделения борьбы с киберпреступностью.

Изложение основного материала исследования. Следует отдать должное японским криминологам и специалистам в области уголовного права, которые предвидели будущее киберпреступности, ее быстрый рост и серьезные проблемы, с которыми столкнется правоприменительная практика. Они указывали, что сложность расследования таких преступлений заставит переосмыслить традиционные основы следствия, для чего потребуется критически проанализировать практику, одновременно находя решения возникающих проблем в расследовании и судебном процессе [1, с. 143].

Как указывают российские исследователи, необходимо также обратить внимание на то, что зарубежные страны с каждым годом увеличивают число служб и ведомств для противодействия киберпреступности, поэтому стоит изучить и перенять их опыт [2, с. 32]. Так, в последние два десятилетия практически во всех странах мира были в той или иной форме созданы подразделения по борьбе с киберпреступностью, в частности во Франции (2000 г.), Великобритании (2001 г.), Филиппинах (2012 г.) [3, с. 266–267]. В Украине Управление по борьбе с киберпреступностью МВД Украины как отдельное подразделение начало функционировать в 2011 г.

Нормативно-правовую базу борьбы с киберпреступностью в Украине составляют Конституция Украины, в ст. 17 которой отмечается, что обеспечение информационной безопасности Украины является важнейшей функцией государства, делом всего Украинского народа. Кроме Конституции, положения относительно борьбы из киберпреступностью содержатся в Конвенции «О киберпреступности» от 23.11.2001 г., ратифицированной Верховной Радой Украины 07.09.2005 г. (далее – Конвенция). Кроме Конвенции, к нормативно-правовой базе борьбы с киберпреступностью можно отнести нормы Уголовного кодекса Украины (почти все составы преступлений могут охватывать использование киберпространства для их совершения), Уголовного процессуального кодекса Украины, в частности ст. 263 («Снятие информации с транспортных телекоммуникационных сетей»), ст. 264 («Снятие информации с электронных информационных систем»), ст. 268 («Установление местонахождения радиоэлектронного средства»), ст. 274 («Негласное получение образцов, необходимых для сравнительного исследования»). Большое значение в борьбе с киберпреступностью имеет и Закон Украины «Об оперативно-розыскной деятельности» (ст. 8), а также ряд других законодательных актов, среди которых можно выделить Законы Украины: «О телекоммуникациях», «О защите информации в информационно-телекоммуникационных системах» и тому подобное [4].

Задачи и функции подразделений по борьбе с киберпреступностью отражены в Приказе МВД Украины «Об организации деятельности Управления борьбы с киберпреступностью МВД Украины и подразделений борьбы с киберпреступностью ГУМВД, УМВД» [5]. Данный документ содержит в себе административно-правовые нормы, которые по своему воздействию на отношения, пишет А.Л. Аксенкин, можно отнести к императивным, т. е. содержащим властное предписание, побуждающее субъект действовать или воздерживаться от совершения определенных действий [6, с. 88].

Как указывается в данном Приказе, задачами подразделений борьбы с киберпреступностью является участие в формировании и обеспечении реализации государственной политики по предупреждению и противодействию уголовным правонарушением, механизм подготовки, совершения или сокрытия которых предусматривает использование электронно-вычислительных машин (компьютеров), систем и компьютерных сетей и сетей электросвязи, а также другим уголовным правонарушением, совершенным с их использованием, в том числе следующим:

– уголовным правонарушениям в сфере использования электронно-вычислительных машин (компьютеров), систем и компьютерных сетей и сетей электросвязи;

– уголовным правонарушением, механизм подготовки, совершения или сокрытия которых предусматривает использование электронно-вычислительных машин (компьютеров), систем и компьютерных сетей и сетей электросвязи (в сферах платежных систем; оборота информации противоправного характера с использованием электронно-вычислительных машин (компьютеров), систем и компьютерных сетей и сетей электросвязи; экономики, которая включает в себя финансовые и торговые транзакции, осуществляемые с помощью сетей электросвязи или компьютерных сетей, а также противодействие запрещенным видам хозяйственной деятельности в данной сфере; предоставлению телекоммуникационных услуг; а также мошенничествам и легализации (отмыванию) доходов, полученных от указанных выше уголовных правонарушений).

Основными функциями подразделений борьбы с киберпреступностью являются следующие:

– определение, разработка и обеспечение реализации комплекса организационных и практических мероприятий, направленных на предупреждение и противодействие уголовным правонарушениям, которые отнесены к их компетенции;

– в пределах своих полномочий, в соответствии с законами, которые составляют правовую основу оперативно-розыскной деятельности, осуществление необходимых оперативно-розыскных мероприятий по выявлению причин и условий, которые способствуют совершению уголовных правонарушений, отнесенных к их компетенции, осуществление профилактики данных правонарушений;

– осуществление предусмотренных действующим законодательством мероприятий по сбору и обобщению информации по объектам, которые пред-

ставляют оперативный интерес, в том числе объектов сферы телекоммуникаций, Интернет-услуг, банковских учреждений и платежных систем с целью предупреждения, выявления и пресечения уголовных правонарушений, отнесенных к компетенции подразделений борьбы с киберпреступностью;

– определение основных направлений и тактики оперативно-служебной деятельности в сфере борьбы из киберпреступностью;

– организация изучения материалов по итогам осуществления работниками подразделений борьбы с киберпреступностью оперативно-розыскной деятельности, в том числе дел оперативного учета, материалов выполнения письменных поручений следователя, указаний прокурора и постановлений суда;

– осуществление оперативно-розыскной деятельности, в соответствии с компетенцией, в порядке, предусмотренном законодательством и другими нормативно-правовыми актами;

– осуществление в пределах своих полномочий на основаниях и в порядке, установленном действующим законодательством, мероприятий по быстрому и полному предупреждению, выявлению и пресечению уголовных правонарушений по направлениям деятельности подразделений борьбы с киберпреступностью;

– обеспечение в порядке, предусмотренном действующим законодательством, создание и применение автоматизированных информационных систем (формирование и пополнение информационных массивов данных), в соответствии с потребностями оперативно служебной деятельности;

– выполнение поручений следователя, прокурора относительно проведения следственных (розыскных) действий и негласных следственных (розыскных) действий в уголовных производствах, которые относятся к компетенции подразделений борьбы с киберпреступностью;

– осуществление текущего и перспективного планирования своей работы;

– по согласованию с руководством МВД организация проведения комплексных и целевых оперативно-профилактических мероприятий, в том числе при участии правоохранительных органов других стран;

– внесение в установленном порядке предложений относительно совершенствования законодательной базы в сфере борьбы из киберпреступностью, а также участие в разработке и прорабатывании проектов законодательных и других нормативно-правовых актов в данной сфере;

– сбор, обобщение, систематизация и анализ информации о криминогенных процессах и состоянии борьбы с уголовными правонарушениями по приоритетным направлениям деятельности подразделений борьбы с киберпреступностью.

Как видим, соответствующие функции подразделений борьбы с киберпреступностью можно разделить на несколько групп:

– оперативно-розыскные;

– организационные;

– методические;

– аналитические.

Важным вопросом, отражающим компетенцию сотрудников подразделений борьбы с киберпреступностью, является определение места совершения киберпреступления, что во многом есть определяющим в юрисдикционном плане.

В.В. Степанов-Егинянц считает, что вопросы о месте совершения компьютерных преступлений и применимом праве в отношении этого вида преступных деяний решаются каждый раз индивидуально. Этим и объясняется сложность международно-правового взаимодействия правоохранительных органов. По его мнению, при совершении транснационального преступления расследование может относиться к компетенции страны, в которой находился преступник в момент совершения им общественно опасного деяния. В случае наступления общественных опасных последствий в третьих странах вопрос о привлечении к уголовной ответственности должен решаться по соглашению государств с учетом соблюдения общепризнанного правового принципа non bis in idem и в тесном сотрудничестве со страной, которой причинен ущерб. С другой стороны, если неизвестно лицо, совершившее преступление, но известно потерпевшее лицо, расследование должны начинать на территории государства, в котором действует потерпевший [7, с. 19]. Вопросы юрисдикции в борьбе с киберпреступностью также поднимал А.В. Манжай [8, с. 218]. Тем не менее данный вопрос остается наиболее сложным для правоохранительных органов не только Украины, но и всего мира.

В этой связи представляется актуальным мнение А.Б. Попова, который считает, что тенденция роста киберпреступности и тенденция «отставания» социально-правового контроля над ней увязываются в некий порочный круг, разорвать который можно только путем органичного сочетания уголовно-правовых и криминалистических стратегий борьбы с данным видом преступлений. Причем важной составляющей такой стратегии должно стать международное сотрудничество в этой сфере, поскольку уже очевидно, что контролировать транснациональную составляющую киберпреступлений на уровне отдельных государств практически невозможно. Международное сотрудничество в борьбе с преступностью в сфере использования компьютерных технологий нуждается в наличии правового, организационного и научного обеспечения [9, с. 312–313].

На необходимости активизации международного сотрудничества указывают также В.А. Номоконов и Т.Л. Тропина, отмечая при этом, что контролировать киберпреступность и бороться с ней на уровне отдельного государства практически невозможно [10, с. 54]. Причем следует иметь в виду, что в силу отсутствия территориальных границ в Интернете любая инициатива, объединяющая страны для борьбы с киберпреступностью по территориальным, политическим или иным признакам, заведомо ограничивает себя рамками, которые не позволят эффективно реализовывать задачи по противодействию киберкриминалитету [11, с. 128].

Борьба с киберпреступностью подразумевает различные подходы. Как отмечают О.Э. Згадзай, С.Я. Казанцев, просматриваются два принципиальных направления:

1) максимально эффективное предупреждение, профилактика, предотвращение самой возможности правонарушений;

2) ориентация на выявление и пресечение совершенных преступных деяний [12, с. 85].

По нашему мнению, первое направление в работе подразделений борьбы

с киберпреступностью должно быть приоритетным. В этой связи хотелось бы отметить следующее. Как верно указывают Н.В. Цалко и Н.Е. Мерецкий, международный опыт борьбы с преступностью свидетельствует о том, что одним из приоритетных направлений решения задачи эффективного противодействия современной преступной деятельности является активное использование правоохранительными органами различных мер профилактического характера [13, с. 297]. Принятие в Украине в 2012 г. Уголовного процессуального кодекса формально закрепило усиление предупредительной составляющей в борьбе с преступностью. Среди прочего это отразилось в переориентации института оперативно-розыскной деятельности на выявление и предупреждение преступлений.

Тем не менее система предупреждения киберпреступлений в Украине нуждается в усовершенствовании, в частности требует решения вопрос построения национальной системы кибербезопасности (см., например, [14], [15]), в которой подразделения борьбы с киберпреступностью, по нашему мнению, должны играть ключевую роль. Д.Н. Карпова указывает, что для эффективного противодействия виртуальным преступникам необходима многоуровневая институциональная система кибербезопасности, которая защищала бы и простых граждан, и государственные институты. Система кибербезопасности включает в себя многообразные компоненты, в т. ч. повышение уровня цифровой грамотности населения, содействие в продвижении индивидуальных способов защиты личной информации, механизмы по противодействию и профилактике киберугроз [16, с. 48]. На проблемах профилактики акцентирует внимание и И.Г. Чекунов, который считает, что систематическое проведение профилактической работы среди граждан, направленной на повышение уровня информационной безопасности, будет способствовать решению проблемы роста киберпреступлений [17, с. 102].

Также остается нерешенным вопрос урегулирования оперативно-розыскных полномочий подразделений борьбы с киберпреступлениями в компьютерных сетях. А.В. Манжай и А.В. Винаков правильно предлагают в этой связи разработать и принять Инструкцию МВД Украины «О сетевой активности оперативных работников органов внутренних дел Украины». Среди прочего ими предложено отдельными разделами урегулировать порядок получения информации из сетевых ресурсов, осуществления коммуникаций, создание и использование ненастоящих (имитационных) средств, международной деятельности и т. д. [18].

Кроме того, следует отметить и необходимость делегирования подразделениям борьбы с киберпреступностью при наличии определенных условий некоторых полномочий оперативно-технических подразделений. Это обусловлено тем, что по ряду киберпреступлений нередко возникает потребность стремительного проведения комплекса оперативно-технических мероприятий. Однако несовершенная система внутреннего взаимодействия в органах внутренних дел часто не позволяет своевременно осуществить задуманное, что приводит к потере доказательственной информации по киберпреступлениям. Последние, в свою очередь, как известно, характеризуются неустойчивостью следовой картины.

Выводы. Подводя итог, следует отметить, что, несмотря на достаточно обширный перечень соответствующих функций подразделений борьбы с киберпреступностью в Украине, они, по нашему мнению, не в полной мере отражают их потребности для эффективного противодействия высокотехнологичным преступлениям и нуждаются в усовершенствовании. В частности, требуется расширить и упростить порядок международного взаимодействия указанных подразделений, внеся изменения в соответствующие подзаконные акты. Сами подразделения борьбы с киберпреступностью в лице соответствующего Управления МВД Украины должны играть ключевую роль в построении национальной системы кибербезопасности. Для упорядочения работы в киберпространстве оперативно-розыскными подразделениями необходимо разработать соответствующую инструкцию в системе МВД Украины. Также требуется расширить полномочия подразделений по борьбе с киберпреступностью, в определенных случаях разрешив им проведение оперативно-технических мероприятий.

Список использованной литературы:

1. Морозов Н.А. Борьба с компьютерной преступностью в Японии / Н.А. Морозов // Общество и право. – 2014. – № 2 (48). – С. 141–145.

2. Протасевич А.А. Борьба с киберпреступностью как актуальная задача современной науки // А.А. Протасевич, Л.П. Зверянская // Криминологический журнал ОГУЭП. – 2011. – № 3 (17). – С. 28–33.

3. Оперативно-розшукова компаративістика : [монографія] / [О.М. Бандурка, М.М. Перепелиця, О.В. Манжай та ін.]. – Х. : Золота миля, 2013. – 352 с.

4. Манжай О.В. Проблеми нормативно-правового забезпечення боротьби з кіберзлочинністю в Україні / О.В. Манжай // Форум права. – 2013. – № 1. – С. 646–650. – [Електронний ресурс]. – Режим доступу : http://archive.nbuv.gov.ua/e-journals/FP/2013-1/13movkvu.pdf.

5. Про організацію діяльності Управління боротьби з кіберзлочинністю МВС України та підрозділів боротьби з кіберзлочинністю ГУМВС, УМВС : Наказ МВС України від 30.10.2012 р. № 988 [Електронний ресурс]. – Режим доступу : http://document.ua/pro-organizaciyu-dijalnosti-upravlinnja-borotbi-z-kiberzloch-doc130740.html.

6. Аксенкин А.Л. Норма права как основное средство административно-правового регулирования противодействия пропаганде наркотических средств, психотропных веществ и их прекурсоров в сети Интернет // А.Л. Аксенкин // Среднерусский вестник общественных наук. – 2012. – № 1. – С. 87–91.

7. Степанов-Егиянц В.Г. К вопросу о месте совершения компьютерных преступлений / В.Г. Степанов-Егиянц // Армия и общество. – 2014. – № 5 (42). – С. 16–20.

8. Манжай О.В. Використання кіберпростору в оперативно-розшуковій діяльності / О.В. Манжай // Право і безпека. – 2009. – № 4 (31). – С. 215–219.

9. Попов А.Б. Международное сотрудничество государств в борьбе с компьютерной преступностью / А.Б. Попов // Вестник Тамбовского университета. Серия «Гуманитарные науки». – 2010. – № 4 (84). – С. 310–313.

10. Номоконов В.А. Киберпреступность как новая криминальная угроза / В.А. Номоконов, Т.Л. Тропина // Криминология: вчера, сегодня, завтра. – 2012. – № 24. – С. 45–55.

11. Кузнецов М.А. Киберпреступность в России / М.А. Кузнецов, А.А. Тигашева // Основные тенденции развития Российского законодательства. – 2012. – № 7. – С. 127–128.

12. Згадзай О.Э. Киберпреступность: факторы риска и проблемы борьбы / О.Э. Згадзай, С.Я. Казанцев // Вестник НЦБЖД. – 2013. – № 4 (18). – С. 80–86.

13. Цалко Н.В. Преступления в сфере высоких технологий экономической направленности / Н.В. Цалко, Н.Е. Мерецкий // Научно-техническое и экономическое сотрудничество стран АТР в XXI веке. – 2012. – Т. 3. – С. 293–299.

14. Носов В.В. Організація та забезпечення інформаційної безпеки : [навчальний посібник] / В.В. Носов, О.В. Манжай. – Х. : Вид-во Харк. нац. ун-ту внутр. справ, 2007. – 216 с.

15. Манжай О.В. Правові засади захисту інформації : [навчальний посібник] / О.В. Манжай. – Х. : Ніка Нова, 2014. – 104 с. – з іл.

16. Карпова Д.Н. Киберпреступность: глобальная проблема и ее решение / Д.Н. Карпова // Власть. – 2014. – № 8. – С. 46–50.

17. Чекунов И.Г. Киберпреступность: проблемы и пути их решения / И.Г. Чекунов // Вестник Академии права и управления. – 2011. – № 25. – С. 97–103.

18. Манжай О.В. Використання програмного забезпечення для провадження окремих слідчих дій та оперативно-розшукових заходів / О.В. Манжай, А.В. Вінаков // Форум права. – 2012. – № 2. – С. 437–441. – [Електронний ресурс]. – Режим доступу : http://www.nbuv.gov.ua/e-journals/FP/2012-2/12movorz.pdf.