

Чурикова А.Ю.,

DOI 10.51980/2021_1_209

кандидат юридических наук, доцент
Поволжский институт управления – филиал РАНХиГС (г. Саратов)

Противодействие киберпреступности: роль прокурора (уголовно-процессуальный аспект)¹

Вопросы организации противодействия и профилактики киберпреступности являются в настоящее время одними из наиболее актуальных. Согласно только официальной статистике, приводимой Генеральной прокуратурой РФ, «массив преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, за последние 5 лет увеличился более чем в шесть раз с 43,8 тыс. преступлений в 2015 г. до 294,4 тыс. в 2019 г. По итогам первого полугодия 2020 г. их количество возросло почти на 92% (до 225,5 тыс.). Если годом ранее такими деяниями было каждое девятое регистрируемое преступление, то сегодня – это уже каждый пятый факт (22,3%)»². Рост киберпреступности сказывается на всех сферах жизнедеятельности общества и хозяйствующих субъектов по всему миру. Так, согласно данным международных исследований, ущерб от таких преступлений в мировом масштабе превысил 1 триллион долларов³.

Исследователи отмечают международный характер киберпреступности⁴, что обуславливает потребность активного международного сотрудничества при организации противодействия киберпреступлениям, а также при расследовании данных преступлений.

Согласно действующему законодательству, на Генеральную прокуратуру Российской Федерации возложены обязанности по осуществлению международного сотрудничества, в том числе и по вопросам правовой помощи и борьбы с преступностью (ст. 2 Федерального закона от 17 января 1992 г. № 2202-1 «О прокуратуре Российской Федерации»).

Кроме того, именно на прокуроров возложена координация деятельности правоохранительных органов по борьбе с преступностью (ст. 8 Федерального закона «О прокуратуре Российской Федерации»). В вопросах борьбы с преступлениями, совершенными с использованием информационно-телекоммуникационных технологий координация деятельности правоохранительных органов является особенно важным направлением, так как именно благодаря слаженной работе органов следствия, дознания и оперативных подразделений возможно своевременное выявление, пресечение, а также расследование и раскрытие данного вида преступлений.

С целью определения наиболее эффективных способов противодействия киберпреступлениям и роли в этом противодействии прокурора, считаем необходимым провести классификацию, имеющую значение для предотвращения данного вида преступлений. Анализируя

¹ Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 20-011-00887 «Правовая модель деятельности прокурора как основа стратегии реформы уголовного процесса».

² Состояние преступности в России за январь-июнь 2020 года / Генеральная прокуратура Российской Федерации. Главное управление правовой статистики и информационных технологий. Официальный сайт Генеральной прокуратуры Российской Федерации. ГКДЖ https://genproc.gov.ru/upload/iblock/4fb/sbornik_6_2020.pdf (дата обращения: 30.01.2021)

³ Глобальный ущерб от киберпреступности в 2020 году превысил 1 триллион долларов // Информационно-новостной портал. URL: https://evo-rus.com/avto/exluzive/globalnyj-ushherb-ot-kiberprestupnosti-v-2020-godu-prevysil-1-trillion-dollarov.html?utm_source=yxnews&utm_medium=desktop (дата обращения: 30.01.2021).

⁴ См.: Желудков М.А., Попов А.М., Дубровина М.М. Особенности противодействия киберпреступности в России и зарубежных странах // Вестник Волгоградской академии МВД России. 2018. № 3 (46). С. 97-102; Булай Ю.Г., Булай Р.И. Профилактика и противодействие киберпреступности, а также международным киберугрозам // Академическая мысль. 2017. № 1. С. 31-35 и т.д.

правоприменительную практику и научную литературу, мы приходим к выводу, что преступления с использованием информационно-телекоммуникационных технологий можно разделить на две большие группы:

1) преступления, совершаемые лицами, обладающими специальными познаниями в области вычислительных технологий и программирования (кибератаки, преднамеренный вывод из строя информационной инфраструктуры и уничтожение баз данных путем использования специальных вредоносных программ и т.д.);

2) преступления, не требующие для их совершения специальных познаний в области информационных технологий и рассчитанные, как правило, на низкий уровень информированности и информационной грамотности населения (мошенничество, подлог, саботаж и т.д.).

Предлагаемая нами классификация имеет ключевое значение для выработки стратегии противодействия киберпреступности. Если для первой группы принципиально важным является проведение оперативных мероприятий с участием лиц, обладающих специальными познаниями в сфере IT-технологий, то для второй группы в противодействии на первое место выступает профилактическая работа с населением.

То есть для первой группы основным направлением деятельности прокурора в организации противодействия будет выступать координация деятельности правоохранительных органов. Для второй группы прокуроры должны организовать, в первую очередь, высокоэффективные профилактические мероприятия, направленные на повышение уровня информированности и информационной грамотности населения.

Кроме того, в организации противодействия киберпреступности немаловажным является своевременное и неукоснительное привлечение к уголовной ответственности лиц, совершивших данные преступления, что будет невозможным без организации должного уровня уголовного преследования на всех стадиях уголовного процесса.

Таким образом, роль прокурора в противодействии киберпреступности в первую очередь заключается в следующем:

1) координация деятельности правоохранительных органов по выявлению и расследованию киберпреступлений;

2) международное сотрудничество по расследованию киберпреступлений и организация взаимодействия на межгосударственном уровне по борьбе с киберпреступлениями;

3) организация мероприятий, направленных на профилактику киберпреступности и повышение уровня информированности и информационной грамотности населения;

4) организация и поддержание законного и обоснованного уголовного преследования лиц, совершивших киберпреступления.

Однако реализация данных направлений противодействия киберпреступности затруднена целым рядом несовершенств действующего уголовно-процессуального законодательства и нестабильностью правового положения прокурора в уголовном процессе.

С одной стороны, прокурор вытесняется из сферы досудебного производства: его лишили многих полномочий, позволявших ему вмешиваться в ход расследования, непосредственно направлять его, а также обеспечивать законность уголовного преследования, осуществляя надзорные полномочия. С другой – прокурор даже законодательно по-прежнему ключевая фигура досудебного производства: Федеральный закон «О прокуратуре Российской Федерации» возлагает на него координацию деятельности правоохранительных органов, уголовно-процессуальный закон по-прежнему выделяет его как основного субъекта осуществления уголовного преследования (ч. 1 ст. 21 УПК РФ), именно на прокурора возложено международное сотрудничество в уголовном процессе.

Такое правовое положение прокурора является противоречивым, нелогичным, а порою даже абсурдным. Разве возможно координировать деятельность правоохранительных органов по борьбе с

преступностью, не контролируя и не направляя ход расследования по уголовным делам? Разве возможно возглавлять уголовное преследование и нести за него ответственность, не осуществляя полноценного надзора за его законностью и обоснованностью не только в ходе дознания, но и в ходе предварительного следствия?

Такая законодательная непоследовательность и противоречивость породила удивительный факт: нормативное закрепление полномочий прокурора в уголовном судопроизводстве и их фактическая реализация прокурором, выражающаяся в организации взаимодействия с иными компетентными участниками уголовного процесса, существенно различаются. Получается, что прокуроры, проводя координационные совещания, фактически дают указания о направлении хода расследования, что уголовно-процессуальным законом в отношении следствия сейчас не предусмотрено.

Ситуация с ограничением уголовно-процессуальных полномочий прокурора в отношении следствия при отсутствии существенной разницы между следствием и дознанием как формами расследования способствует тому, что деятельность прокурора в уголовном процессе и

его взаимодействие с органами следствия начинают осуществляться вне рамок правового поля, что, в свою очередь, существенно снижает эффективность организации противодействия киберпреступности, так как данные преступления в большинстве случаев расследуются в форме следствия.

Таким образом, мы видим, что прокурор играет значительную роль в противодействии киберпреступности, однако реализация им полномочий, направленных на организацию противодействия и профилактику данного вида преступлений, затруднена в силу существенных недостатков действующего уголовно-процессуального законодательства. В связи с этим считаем необходимым изменить подход к нормативному закреплению модели деятельности прокурора в уголовном процессе. Правовая модель, закрепленная в законодательстве, должна быть построена с учетом правоприменительной практики и потребностей современного общества, то есть необходимо последовательное и логичное закрепление положения прокурора как организатора, руководителя и координатора уголовного преследования на всех стадиях уголовного процесса.