Стегалин Сергей Валентинович
1 курс адъюнктура
Нижегородская академия МВД России

«ПРОБЛЕМА КОМПЛЕКТОВАНИЯ СПЕЦИАЛИЗИРОВАННЫХ ПОДРАЗДЕЛЕНИЙ ОВД РФ ПО РАСКРЫТИЮ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ».

THE PROBLEM OF RECRUITING SPECIALIZED DEPARTMENTS OF THE MINISTRY OF INTERNAL AFFAIRS OF THE RUSSIAN FEDERATION TO SOLVE CRIMES COMMITTED USING INFORMATION AND TELECOMMUNICATION TECHNOLOGIES

Аннотация. Для эффективной борьбы с IT-преступностью требуется наращивание внутренних ресурсов правоохранительных органов. Достижение положительного эффекта в борьбе с преступлениями в сфере цифровых технологий обусловлено созданием специализированных подразделений МВД России, в том числе в органах предварительного расследования. Стратегически правильное определение задач и функций новых подразделений на уровне МВД России, а также грамотно выстроенная и последовательная управленческая работа руководителя следственного подразделения способны повысить качество раскрытия и расследования преступлений, совершенных с использованием информационно-телекоммуникационных технологий.

Ключевые слова и словосочетания: IT-преступность; информационно-телекоммуникационные технологии; киберпреступление; специализированное подразделение; специализированная следственно-оперативная группа.

Annotation. In order to effectively combat IT crime, it is necessary to increase the internal resources of law enforcement agencies. The achievement of a positive effect in the fight against crimes in the field of digital technologies is due to the creation of specialized units of the Ministry of Internal Affairs of Russia, including in the bodies of preliminary investigation. Strategically correct definition of the tasks and functions of new units at the level of the Ministry of Internal Affairs of Russia, as well as well-structured and consistent managerial work of the head of the investigative unit can improve the quality of disclosure and investigation of crimes committed using information and telecommunication technologies.

Keywords and phrases: IT crime; information and telecommunication technologies; cybercrime; specialized unit; specialized investigative task force.

Значимость противодействия IT-преступности неоднократно обозначалась как Президентом Российской Федерации В. В. Путиным, так и руководством МВД России на протяжении последних нескольких лет. Так, 17 февраля 2022 г. на заседании коллегии МВД России, на котором были подведены итоги оперативно-служебной деятельности, Министр внутренних дел Российской Федерации генерал полиции В. А. Колокольцев отметил достигнутый определенный эффект, который дали предложенные министерством меры по предупреждению IT-преступлений [1, с. 19].

Обозначенные В. А. Колокольцевым результаты достигнуты благодаря последовательной работе по улучшению качества раскрытия, расследования преступлений указанной категории следователями системы МВД России. Ученые-криминалисты также отмечают прогресс в этой сфере.

Так, Ю. В. Гаврилин и А. Г. Парадников пишут: «Следует заметить, что в последнее время наметилась позитивная тенденция повышения эффективности деятельности органов внутренних дел в сфере противодействия высокотехнологичной преступности, что является

результатом системной и последовательной работы в данном направлении [2, с. 125].

В рамках реализации решения коллегии МВД России от 1 ноября 2019 г. № 3км в территориальных органах МВД России проведены организационно-штатные мероприятия, итогом которых стало создание как на районном, так и на региональном уровнях специализированных подразделений по расследованию преступлений в сфере информационно-телекоммуникационных технологий (далее – ИТТ).

Кроме создания специализированных подразделений, с учетом отсутствия достаточного количества сотрудников, в ряде регионов издаются приказы о специализации отдельных следователей, которые проводят уголовно-процессуальную проверку, а также последующее расследование преступлений в сфере ИТТ. Расследование же наиболее сложных уголовных дел, по которым установлены лица, совершившие преступления в составе организованной преступной группы, поручается следователям следственных частей ГСУ и СУ.

Практика выделения в структуре следственных подразделений, специализированных не является единой как на региональном, так и на районном уровнях. В ряде регионов Российской Федерации с целью повышения эффективности взаимодействия подразделений органов внутренних дел при раскрытии и расследовании преступлений, совершенных с использованием компьютерных и телекоммуникационных технологий, оперативного сопровождения уголовных дел, оказания территориальным органам МВД России на районном уровне практической и методической помощи в их раскрытии и расследовании, а также выявления признаков серийности и многоэпизодных дел, имеющих межрайонный и межрегиональный характер, реализации мер совместной работы по возмещению ущерба, причиненного преступлениями, создаются рабочие группы по оказанию территориальным органам на районном уровне практической и методической помощи в раскрытии и расследовании

уголовных дел о преступлениях, совершенных с использованием ИТТ (Псковская область, Тверская область, Свердловская область).

В состав рабочих групп включаются сотрудники следственных, оперативных подразделений, подразделений специальных технических мероприятий, отдела дознания, отделов информации и общественных связей, участковых уполномоченных полиции.

Основными задачами подобных рабочих групп в целом является организация взаимодействия структурных подразделений по раскрытию и профилактике преступлений, связанных с хищением денежных средств, совершенных с использованием ИТТ, повышению эффективности проводимых мероприятий, направленных на профилактику и раскрытие преступлений рассматриваемой категории, по своевременному и качественному взаимообмену оперативно значимой информацией.

Кроме того, в целях повышения эффективности работы территориальных органов внутренних дел МВД России на региональном и на районном уровнях по организации и усилению борьбы с хищениями, совершаемыми с использованием ИТТ, а также в целях своевременного, полного, всестороннего и объективного расследования преступлений названной категории существует практика создания специализированных следственно-оперативных групп (далее – ССОГ).

Задачами ССОГ являются: реагирование на своевременное возбуждение уголовных дел по указанной категории преступлений, проведение мониторинга сообщений о преступлениях, совершенных с использованием ИТТ, обеспечение оперативного взаимодействия и обмена информацией, получаемой различными подразделениями, но в первую очередь раскрытие и расследование конкретных уголовных дел.

На необходимость постоянного повышения квалификации и профессионализма сотрудников следственных подразделений, знания которых не всегда достаточны для качественного расследования указанной категории уголовных дел указывают Ю. В. Гаврилин и Я. Р. Реент [3, с. 96].

В целях повышения профессионального уровня следователей вышеуказанных подразделений и ССОГ на постоянной основе проводятся занятия, изучаются методические рекомендации и обзоры, подготовленные Следственным департаментом МВД России, обзоры, подготовленные контрольно-методическими подразделениями по расследованию преступлений обозначенной категории. По мнению А. В. Сибильковой и А. С. Беляева, рациональнее доводить до следователей и специалистов (экспертов) оперативную экспресс-информацию в виде систематической рассылки, а также в ходе дополнительной профессиональной подготовки (стажировок, повышения квалификации) и совместных совещаний посредством видео-конференц-связи. К этой деятельности целесообразно привлекать профессионалов компаний, специализирующихся на информационной безопасности [4, с. 180]. Задачи формирования компетенций по противодействию преступлениям, совершенным с использованием ИТТ на более высоком уровне, решаются в Академии управления МВД России.

Однако только дополнительное создание специализированных подразделений в целях повышения качества борьбы с ИТ-преступностью не обеспечит достижения указанных целей без грамотно выстроенной и организованной управленческой работы руководителя следственного подразделения.

В связи с вышеизложенным организационно-управленческая деятельность руководителя должна включать в себя:

– информационно-аналитическое обеспечение;

– планирование деятельности органов предварительного следствия системы МВД России и их сотрудников;

– организацию принятия и реализации управленческих решений;

– взаимодействие и координацию всех подразделений.

Не менее важное значение имеют и такие составляющие организационной деятельности руководителя следственного подразделения как ресурсное обеспечение, включающее в себя кадровое, материально-техническое и финансовое.

Состав следственно-оперативной группы при расследовании киберпреступлений весьма разнообразен: это специалист-криминалист, специалист по средствам вычислительной техники, сотрудник ФСТЭК России, Центра защиты информации (при обнаружении на месте осмотра конфиденциальной компьютерной информации, машинных носителей, специальных средств защиты от несанкционированного доступа и (или) технических средств негласного получения (уничтожения, блокирования) компьютерной информации), специалист по сетевым технологиям (в случае наличия периферийного оборудования удаленного доступа или локальной компьютерной сети), специалист по системам электросвязи (при использовании для дистанционной передачи данных каналов электросвязи), оперативные сотрудники БСТМ. Также в состав группы могут входить бухгалтеры, специалисты спутниковых систем связи, операторы компьютерных систем и сетей электросвязи и др.

Таким образом, при всех недостатках в деятельности специализированных подразделений, сформированных для раскрытия и расследования преступлений в сфере ИТТ, имеется положительная динамика в борьбе с указанным видом преступности в абсолютных показателях по раскрытию данной категории преступлений и направлению уголовных дел в суд. Следователи и руководители проводят в данном направлении планомерную работу, которая оказывает положительный эффект на конечные результаты.

Для противодействия преступлениям в сфере ИКТ и компьютерных технологий правоохранительные органы должны обладать знанием способов совершения таких преступлений, тактики и методики выявления, раскрытия и расследования преступлений данной категории; стремиться к

превосходству над злоумышленниками в уровне технической оснащенности и скорости получения информации. Особенно актуален данный вопрос при осуществлении противодействия мошенничествам и кражам, совершенным с использованием ИКТ. Однако многие сотрудники ОВД, осуществляющие противодействие преступлениям, совершенным с использованием современных информационно-коммуникационных технологий, сталкиваются с рядом существенных трудностей при получении необходимой информации, что негативно сказывается на итогах оперативно-служебной деятельности.

Кроме того, у сотрудников ОВД, осуществляющим противодействие преступлениям, совершенным с использованием современных информационно-коммуникационных технологий, должны быть сформированы следующие профессиональные компетенции: способен использовать компьютерную технику, справочно-правовые информационные системы, учеты и автоматизированные информационно-поисковые системы при осуществлении служебной деятельности, в том числе с учетом требований информационной безопасности; способен решать задачи служебной деятельности по выявлению, предупреждению, пресечению и раскрытию преступлений и иных правонарушений, в том числе совершаемых с использованием ИТТ; способен осуществлять деятельность по формированию оперативных и иных учетов, использованию информационных ресурсов и технологий для решения задач оперативно-розыскной деятельности.

Совершение ряда преступных деяний не позволяет объективно оценивать масштабы киберпреступности. Сфера кибербезопасности тоже достаточно широкая и сложная, однако правоохранительным органам в ней отведена отдельная и очень важная роль. Преступления требуется фиксировать документально, хотя они существуют в киберпространстве, что заставляет правоохранительную систему учиться использовать новые методы в борьбе с преступностью, разрабатывать способы, которые бы помогали достигать эффективного и быстрого результата в данном вопросе.

МВД активно сотрудничает с этой целью с Роскомнадзором, интернет-провайдерами, Генеральной прокуратурой Российской Федерации, СМИ. Стоит отметить, что последние играют роль информатора, который помогает населению повышать компьютерную грамотность и не попадаться на уловки мошенников.

Важно решить проблему с кадровым дефицитом органов МВД, не только набрать оптимальное число сотрудников, но и обучить их правильной тактике борьбы с преступлениями в сфере информационных технологий. Стоит обратить особое внимание на то, что преступления, совершенные в киберпространстве, не могут быть раскрыты классическими методами расследования. Образовательная система органов МВД должна проводить специальную подготовку по поднятому в данном материале вопросу, обучение также может потребоваться не только будущим, но и действующим сотрудникам.

Основополагающую роль в методике раскрытия кибермошенничества играют тактические приемы проведения следственных действий. Стоит обратить внимание на то, что данный вид преступной деятельности весьма специфический. Для его раскрытия сотрудники правоохранительных органов должны иметь соответствующие знания. Часто следователь не может выстроить правильную линию допроса из-за отсутствия таких знаний. Из-за этого у мошенника появляется возможность запутать следствие, используя специфические знания, которыми он обладает.

Этот же момент можно отнести к проведению судебной экспертизы. Часто следователь не обладает достаточно глубокими знаниями в вопросе кибермошенничества и не может правильно поставить вопросы перед экспертом. Это не позволяет получить исчерпывающий или точный ответ.

Для решения этой проблемы необходимо обучение следователей специфической методике раскрытия киберпреступлений. Сотрудник следственных органов должен хорошо представлять, что такое киберпространство, как это работает, иметь в этой области высокую

квалификацию, уметь правильно ставить вопросы перед обвиняемым и экспертом, разбираться в специфических терминах, понимать механизмы работы в киберпространстве. Такой подход обеспечит более качественное проведение допросов и иных следственных действий.

Совершенствование методик выражается не только в повышении уровня знаний сотрудников правоохранительных органов, но и улучшении технического обеспечения, появлении новых криминалистических лабораторий, способных осуществлять экспертизу.

Список используемой литературы и используемых источников

1. Вестник МВД России. Спецвыпуск 2/3. Москва 2022.

2. Гаврилин Ю.В., Парадников А.Г. Совершенствование выявления, раскрытия и расследования хищений, совершенных и использованием информационных банковских технологий (по итогам всероссийского онлайн-семинара) // Труды Академии управления МВД России. 2020. № 2 (54). С. 123-129.

3. Гаврилин Ю.В., Реент Я.Р. Обеспечение начальником территориального органа МВД России на районном уровне раскрытия и расследования преступлений, совершенных с использованием информационно-телекоммуникационных технологий // Академическая мысль. 2021. № 4 (17). С. 94-98.

4. Сибилькова А.В., Беляев А.С. Обеспечение начальником территориального органа МВД России специальных знаний при раскрытии и расследовании преступлений, совершенных с использованием IT-технологий // Академическая мысль. № 2 (19) 2022. С. 179-182.