Матвеев А.В.,

кандидат юридических наук
Ленинградский областной филиал
Санкт-Петербургского университета МВД России (п. Мурино)

Совершенствование профессиональной подготовки сотрудников органов внутренних дел как условие эффективности противодействия киберпреступности

В связи с приобретением информационными технологиями глобального трансграничного характера и внедрением их во все сферы деятельности личности, общества и государства, одним из приоритетных направлений деятельности правоохранительной системы государства на современном этапе становится повышение эффективности противодействия преступлениям, совершаемым с использованием информационных технологий[1].

Невзирая на актуальность противодействия рассматриваемой категории преступлений, понятие преступления, совершенного с использованием информационных технологий (далее – киберпреступление), в настоящее время юридической наукой не выработано и положениями действующего законодательства не закреплено. В настоящем исследовании понятие киберпреступления рассматривается в рамках подхода, предложенного учеными-исследователями ВНИИ МВД России И.Б. Колчевским и Г.Э. Бицадзе, которые сформулировали понятие киберпреступления как противоправного общественно опасного деяния, причиняющего вред разнородным общественным отношениям, совершаемого с использованием информационных технологий, информационных систем, информационно-телекоммуникационных сетей[2].

Об особой актуальности принятия мер по противодействию киберпреступлениям свидетельствуют статистические данные. Согласно характеристике состояния преступности в Российской Федерации за январь – ноябрь 2024 года, в Российской Федерации за указанный период зарегистрированы 702 923 киберпреступления, что на 14,3% больше, чем за аналогичный период 2023 года. В общем числе зарегистрированных преступлений их удельный вес увеличился с 34,1% в январе-ноябре 2023 года до 39,9%. Почти половина киберпреступлений относится к категориям тяжких и особо тяжких, четыре преступления из пяти совершаются с использованием сети Интернет, почти половина – средств мобильной связи. Подавляющее большинство совершаемых киберпреступлений (98,7%) выявляется органами внутренних дел[3].

Приведенные статистические данные одновременно свидетельствуют о стремительном развитии киберпреступности, наличии острой необходимости в противодействии киберпреступлениям и о ведущей роли органов внутренних дел как субъекта борьбы с рассматриваемой категорией преступлений среди иных правоохранительных органов.

Несмотря на активное участие органов внутренних дел во взаимодействии с другими правоохранительными ведомствами в выявлении и раскрытии киберпреступлений, показатель раскрываемости рассматриваемой категории преступлений является низким – 24,4%[4]. В качестве основных причин низкого уровня раскрываемости киберпреступлений следует выделить низкий уровень информационной и финансовой грамотности населения, недостаточность технического и технологического обеспечения органов внутренних дел, а также отсутствие у сотрудников органов внутренних дел необходимого для эффективного раскрытия киберпреступлений уровня профессиональной подготовки[5].

[1] Об утверждении Доктрины информационной безопасности Российской Федерации : Указ Президента РФ от 05.12.2016 № 646 // Собрание законодательства Российской Федерации. 2016. № 50. Ст. 7074.

[2] Колчевский И. Б., Бицадзе Г. Э. Преступления в сфере информационных технологий: понятие, структура // Научный портал МВД России. 2021. № 2(54). С. 40-47.

[3] Состояние преступности в России за январь-ноябрь 2024 года. URL: https://мвд.рф/reports/item/59951540/ (дата обращения: 17.01.2025).

[4] Там же.

[5] См.: Шхагапсоев З.Л. О некоторых факторах, препятствующих эффективному раскрытию и расследованию преступлений, совершаемых в киберпространстве // Вестник экономической безопасности. 2021. № 2. С. 258–263; Михайлова И.А., Лимарь А.С., Гилаев Р.И. О деятельности правоохранительных органов по противодействию

Вопрос необходимости достижения высокого уровня профессиональной подготовки сотрудников органов внутренних дел по раскрытию киберпреступлений представляется особо актуальным ввиду того, что деятельность по раскрытию киберпреступлений зачастую требует от сотрудников органов внутренних дел специальных познаний в области информационных технологий. В силу того, что должностные лица органов внутренних дел, на которых возложены полномочия по раскрытию киберпреступлений, в большинстве случаев имеют юридическое образование, процедура раскрытия узконаправленных киберпреступлений усложняется для них в связи с необходимостью изучения новой терминологии, процессов и алгоритмов, характерных для стремительно развивающейся сферы информационных технологий, привлечения технических специалистов, что, в свою очередь, способствует увеличению времени необходимого для раскрытия преступления и, как следствие, снижает уровень эффективности противодействия киберпреступности в целом. Высокие темпы развития информационных технологий и недостаточный уровень профессиональной подготовки сотрудников заставляют органы внутренних дел выступать в роли догоняющего по отношению к киберпреступникам, постоянно видоизменяющим способы и внедряющим новые схемы совершения киберпреступлений.

На сегодняшний день органами внутренних дел принимается ряд мер, направленных на совершенствование профессиональной подготовки сотрудников, специализирующихся на противодействии киберпреступности, в частности подготовка в ведомственных университетах кадров по техническим и юридическим специальностям, обладающих компетенциями в сфере противодействия киберпреступлениям[1]. Вместе с тем статистика совершаемых киберпреступлений и низкий уровень их раскрываемости упрямо свидетельствуют о недостаточности принимаемых мер в данной области.

Таким образом, недостаточный уровень профессиональной подготовки сотрудников органов внутренних дел выступает одним из ключевых факторов низкого уровня раскрываемости киберпреступлений, что, в свою очередь, свидетельствует о совершенствовании и повышении уровня профессиональной подготовки сотрудников органов внутренних дел как о важнейшем условии достижения эффективности в противодействии киберпреступности. В целях совершенствования уровня профессиональной подготовки сотрудников органов внутренних дел по противодействию киберпреступности представляется целесообразным принятие мер по разработке и реализации новых, отвечающих вызовам стремительно и непрерывно развивающихся информационных технологий, программ повышения квалификации и профессиональной переподготовки по вопросам борьбы с киберпреступлениями как на базе ведомственных образовательных организаций МВД России, так и в сторонних организациях, осуществляющих образовательную деятельность.

Байкин Р.Ф.

Сибирский юридический институт МВД России (г. Красноярск)

Особенности патриотического воспитания молодежи новых субъектов Российской Федерации и участие обучающихся образовательных организаций МВД России в данном процессе

Воспитание патриотизма выступает в ипостаси значимого способа укрепления единства и целостности для многонационального и мультисубъектного государства как Российская Федерация. Формирование чувства патриотизма населения, в особенности молодежи, представляет собой общественную важность, так как это способствует объединению российского общества, сплочения его для решения острых социальных проблем. В настоящее время политика, направленная на реализацию жизненных интересов

преступлениям, совершаемым в сфере информационно-телекоммуникационных технологий // Вестник экономики, права и социологии. 2024. № 2. С. 109–114.

[1] Информация о противодействии ИТТ-преступлениям. URL: https://гурлс.мвд.рф/направления-деятельности/podgotovka-kadrov/информация-о-противодействии-итт-преступ (дата обращения: 18.01.2025).