При наличии признаков, указывающих на то, что в отношении лица, пропавшего без вести, было совершено общественно опасное деяние, т. е. в ситуациях, при которых сведения о криминальном характере исчезновения лица имеются, основанием для проведения ОРМ являются сведения о подготавливаемом, совершаемом или совершенном преступлении, а также о гражданине, его подготавливающем, совершающем или совершившем либо осведомленном о нем, закрепленные в абзаце третьем части первой ст. 16 Закона об ОРД, во всех иных указанных ситуациях основанием для проведения ОРМ являются сведения о гражданине, без вести пропавшем, закрепленные в абзаце седьмом части первой ст. 16 Закона об ОРД.

Анализ юридической литературы показал, что к лицам, пропавшим без вести, относят исчезнувших внезапно без видимых к тому причин граждан, местонахождение и судьба которых неизвестны. В специальном правовом акте МВД Республики Беларусь, имеющем ограничительный гриф, закреплено определение термина «лицо, пропавшее без вести», под которым понимается физическое лицо, в отношении которого в органы внутренних дел поступило заявление (сообщение) об его исчезновении. Исходя из приведенных определений, можно сделать вывод, что речь о совершенном преступлении в данном случае не ведется. Перечисленные обстоятельства указывают на то, что в ситуации безвестного исчезновения гражданина основание для проведения ОРМ, закрепленное в абзаце четвертом части первой ст. 16 Закона об ОРД (поручение, указание, постановление органа уголовного преследования по уголовному делу, рассматриваемому заявлению или сообщению о преступлении), отсутствует.

Согласно ст. 6 Закона об ОРД оперативно-розыскная деятельность осуществляется на основе Конституции Республики Беларусь. В силу ряда положений Основного Закона государство определило высшей ценностью и своей целью обеспечение защиты прав и свобод человека и гражданина и гарантии их реализации (ст. 2, 21).

Гарантии защиты прав и свобод человека и гражданина должны распространяться в равной мере и на случаи, когда законодателем установлены допустимые ограничения, касающиеся этих прав, что приобретает особое значение в сфере оперативно-розыскной деятельности. При проведении ряда ОРМ затрагиваются права, свободы и законные интересы физических и юридических лиц, в связи с чем законодателем установлен определенный порядок их проведения.

Таким образом, следует отметить, что в основании, закрепленном в абзаце четвертом части первой ст. 16 Закона об ОРД (поручение, указание, постановление органа уголовного преследования по уголовному делу, рассматриваемому заявлению или сообщению о преступлении), речь идет непосредственно о преступлении, а не о факте безвестного исчезновения лица, принятое решение о применении указанного основания в оперативно-служебных документах в рассматриваемых нами оперативно-розыскных ситуациях нарушает принципы законности при осуществлении оперативно-розыскной деятельности, а также соблюдения прав, свобод и законных интересов граждан, закрепленных ст. 6 и 7 Закона об ОРД.

УДК 343 + 342.9(075)

Р.Н. Ключко

УГОЛОВНО-ПОЛИТИЧЕСКИЕ ЗАДАЧИ ОХРАНЫ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ И ПРОТИВОДЕЙСТВИЯ ДЕСТРУКТИВНОМУ ИНФОРМАЦИОННОМУ ВОЗДЕЙСТВИЮ

Важным направлением современной уголовной политики является государственная деятельность по обеспечению уголовно-правовой охраны информационной безопасности личности, общества, государства. Необходимость совершенствования уголовной политики в сфере охраны информационной безопасности, имеющей целью разработку стратегии и тактики борьбы с информационной преступностью, обусловлена стремительным развитием информационных и коммуникационных процессов, появлением новых технологий, а соответственно, новых вызовов и угроз. В последние 20 лет информационная безопасность стала важным стратегическим национальным приоритетом.

Уголовная политика в области обеспечения информационной безопасности, реализуемая в правотворчестве, правоприменении, правовом воспитании, формировании правосознания и в целом в правовой культуре общества, основана на определенном государством ценностно-ориентационном векторе развития общественных отношений в информационной сфере. Первостепенное уголовно-политическое значение имеет определение сферы уголовно-правового регулирования информационных отношений, объема и содержания криминализации деяний для обеспечения информационной безопасности личности, общества, государства, легитимации правовых ограничений доступа к информации и свободы ее распространения.

В общей структуре уголовной политики в сфере обеспечения информационной безопасности можно выделить уголовную политику в сфере обеспечения компьютерной безопасности (кибербезопасности) и информационно-психологической безопасности физических и юридических лиц, общества, государства от внешних и внутренних угроз в информационной сфере, создаваемых посредством общественно опасного информационного воздействия на индивидуальное и общественное сознание либо непредоставления (сокрытия) информации. В настоящее время обеспечение прав и законных интересов, безопасности акторов информационного оборота требует определения границ информационной деятельности, социальных и правовых оснований уголовно-правовых запретов на совершение информационных деяний, разработки научно обоснованных критериев криминализации деяний в виде деструктивного информационного воздействия. Модернизация правовых рамок обеспечения информационной безопасности на различных уровнях (индивидуальный, коллективный, национальный, международный) должна осуществляться на основе разработанной стратегии борьбы с информационной преступностью с учетом потребностей обеспечения прогрессивного общественного развития в условиях нарастания давления технологиче-

ских трансформаций, требующих использования всего спектра средств правового реагирования на возникающие угрозы в информационной сфере.

Проблемы уголовно-правовой охраны кибербезопасности (компьютерной безопасности) с 90-х гг. XX в. являются предметом пристального анализа отечественных ученых-криминалистов. Однако в белорусской уголовно-правовой доктрине почти не уделялось внимание комплексному исследованию проблем информационной безопасности в гуманитарном аспекте, анализу средств и способов уголовно-правового обеспечения информационно-психологической безопасности. Актуальность обращения к проблемам уголовно-правовой охраны информационно-психологической безопасности субъектов информационных отношений обусловлена динамикой политических, экономических, социальных процессов, резким возрастанием значения информации и знаний в условиях развития информационных и коммуникационных технологий, что подтверждается не только отечественными, но и мировыми тенденциями трансформации правового механизма обеспечения информационного суверенитета государства и информационно-психологической безопасности субъектов всех уровней (личный, корпоративный, государственный). Концепция информационной безопасности Республики Беларусь, утвержденная постановлением Совета Безопасности Республики Беларусь от 18 марта 2019 г. № 1, определяет противодействие деструктивным информационно-психологическим воздействиям на массовое общественное сознание в качестве одного из средств обеспечения безопасности информационно-психологической компоненты информационной сферы. Развитие социальных процессов в информационной среде, изменение условий социального бытия, важной сферой которого становится информационная сфера, требуют адаптации как регулятивных, так и охранительных механизмов обеспечения стабильности и прогрессивного развития информационной сферы прав и интересов субъектов информационных отношений.

Концепция в качестве угроз в информационно-психологической сфере определяет действия по дискредитации конституционных основ государства и его властных структур, размыванию национального менталитета, вовлечению людей в экстремистскую и террористическую деятельность, разжиганию межнациональной и межконфессиональной вражды, формированию радикального и протестного потенциала, действия, направленные на нарушение территориальной целостности государства. Мощным фактором психоманипуляции в современной действительности стало умалчивание и фальсификация исторических фактов, изменение трактовок важнейших исторических событий. В этой связи актуальным направлением правовой политики государства становится противодействие трансформации исторической памяти народа, представляющей угрозу национальной безопасности. Деструктивное информационное воздействие используется как метод социального управления и создает угрозу причинения вреда личным, корпоративным, общественным, государственным интересам. Анализ социальной действительности, обусловливающей трансформацию законодательства, свидетельствует о том, что получает распространение информационное воздействие как вид общественно опасного деяния. Указанное предопределяет необходимость дефинирования информационного воздействия как вида информационного деяния, которое выражается в распространении либо предоставлении, а также утаивании, сокрытии, непредоставлении информации с целью оказания влияния на индивидуальное либо групповое сознание.

Анализ актов деструктивного информационного воздействия, свидетельствующий о расширении спектра информационных угроз, указывает на необходимость определения системы правовых средств противодействия таковым на основе научно обоснованной стратегии правовой охраны национальных интересов в информационной сфере. Самостоятельными задачами совершенствования уголовно-правового механизма обеспечения информационной безопасности как интегративного объекта правовой охраны, полагаем, являются:

определение социальной потребности установления уголовной ответственности за общественно опасные информационные деяния;

определение предмета и пределов уголовно-правовой охраны информационной безопасности личности, общества, государства с постулированием ее как важнейшего базового объекта уголовно-правовой охраны;

совершенствование мер уголовно-правового контроля за преступностью в информационной сфере.

УДК 343.985.8

Б.В. Ковалик

МЕХАНИЗМ СОВЕРШЕНИЯ МОШЕННИЧЕСКИХ ДЕЙСТВИЙ ДИСТАНЦИОННЫМ СПОСОБОМ

Одним из наиболее распространенных преступлений, совершаемых в сети Интернет, является мошенничество. Актуальность данной проблемы обостряется формированием транснациональных организованных преступных групп в этой сфере, как правило действующих из-за пределов страны проживания жертв данных преступлений. Алгоритм их функционирования отлажен, и по своей структуре они сходны с действующими на законной основе организациями со своими службами поддержки и безопасности, бухгалтерией и т. д. Большинство из них используют идентичные принципы организации, схемы совершения преступлений и имеют четко выстроенную иерархию.

Площадкой для реализации преступных намерений могут стать классифайды, социальные сети, сайты знакомств и другие интернет-ресурсы. В ходе переписки непосредственный исполнитель просит потенциальную жертву перейти по предоставленной ссылке и выполнить условия рекомендуемого им сервиса, который является фишинговым. Большинство площадок по размещению объявлений препятствуют деятельности мошенников, блокируя сторонние ссылки во внутренних чатах.