УДК 343.431: 343.985

ОПЕРАТИВНО-РОЗЫСКНОЕ ПРОТИВОДЕЙСТВИЕ МОШЕННИЧЕСТВАМ, СОВЕРШЕННЫМ ЧЕРЕЗ СЕТЬ ИНТЕРНЕТ В УКРАИНЕ

Виталий ТЕЛИЙЧУК,
кандидат юридических наук, старший научный сотрудник, доцент,
доцент кафедры оперативно-розыскной деятельности факультета подготовки специалистов
для подразделений криминальной полиции
Днепропетровского государственного университета внутренних дел

Дарья ГОРЕЛИК,
соискатель высшего образования факультета подготовки специалистов для подразделений криминальной полиции
Днепропетровского государственного университета внутренних дел

АННОТАЦИЯ

В статье рассмотрено оперативно-розыскное противодействие интернет-мошенничествам, определены основные направления выявления и оперативно-розыскного предотвращения. Определены основные способы совершения мошенничества в сети Интернет как в Украине, так и за рубежом. Охарактеризовано мошенничество с криптовалютами и в Украине, и в такой развитой стране, как США. Предложены типовые алгоритмы действий сотрудников оперативных подразделений в процессе досудебного расследования, в частности, при осуществлении негласных следственных (розыскных) действиях. Анализируя мнения и доводы ученых в области криминального процесса, криминалистики и оперативно-розыскной деятельности, авторы сделали соответствующие выводы и предложения по усовершенствованию оперативно-розыскного предупреждения указанных видов преступлений.

Ключевые слова: оперативно-розыскное противодействие, мошенничество, сеть Интернет, следственные подразделения, выявление, предотвращение, профилактика.

OPERATIONAL-SEARCH COUNTERACTION TO FRAUD COMMITTED THROUGH THE INTERNET NETWORK IN UKRAINE

Vitaliy TELIYCHUK,
Candidate of Law Sciences, Senior Researcher, Associate Professor,
Associate Professor at the Department of Operatively-Search Activity
of Faculty of Preparation of Experts for Subdivisions of Criminal Police
of Dnepropetrovsk State University of Internal Affairs

Daria GORELIK,
Applicant for Higher Education of Faculty of Training Specialists for Criminal Police Units
of Dnepropetrovsk State University of Internal Affairs

SUMMARY

The article discusses the operational-search counteraction to Internet frauds, identifies the main directions of detection and operational-search prevention. The authors identified the main ways of committing fraud on the Internet, both in Ukraine and abroad. Cryptocurrency fraud has been characterized in Ukraine, and in such a developed country as the United States. Typical algorithms for actions of employees of operational units in the process of pre-trial investigation, in particular during the implementation of covert investigative (search) actions, are proposed. Analyzing the opinions and arguments of scientists in the field of criminal process, criminalistics and operational-search activities, the relevant conclusions and suggestions are made to improve the operational-search prevention of these types of crimes.

Key words: operative search counteraction, fraud, Internet, investigative units, detection, prevention, prevention.

Постановка проблемы. Неотложность изучения вопросов противодействия мошенничествам в сети Интернет в Украине обусловлена рядом объективных факторов. Прежде всего это рост количественных показателей данного вида преступности, которые в сочетании с разнообразием совершения делают проблему деятельности организованных преступных организаций в сфере высоких технологий такой, которая требует неотложного решения. Противодействие мошенничествам оперативно-розыскными мероприятиями включает систему оперативно-розыскных и других мероприятий, реализуется в отдельных организационно-тактических формах. Одной из них является оперативно-розыскное предотвращение таких преступлений, которое фактически представляет собой форму реализации концепции философов-гуманистов о том, что лучше предотвратить преступления, чем наказывать за их совершение. Фактически обозначенная форма оперативно-розыскной деятельности (далее – ОРД) является реализацией мировых стандартов и требований Конституции Украины касательно обеспечения

органами государственной власти соблюдения законов, охраны общественного порядка, прав и законных интересов граждан. С учетом того, что оперативно-розыскная стратегия является составной государственной стратегии противодействия преступности вообще, оперативно-розыскное предупреждение указанных преступлений следует рассматривать как составляющую предупредительной деятельности государства.

Актуальность темы исследования. В современном мире компьютер стал одним из самых распространенных средств общения людей, хранения, создания, сбора, обработки и использования информации в любой области деятельности человека. Стремительное развитие использования сети Интернет в качестве поставщика товара и различных услуг, соответственно, сферы денежного обращения привело к тому, что все большее количество населения Украины становится жертвами мошенничеств, совершенных с использованием сети Интернет. С учетом изложенного и требований законодательства Украины, в частности Конституции Украины, Уголовного, Уголовного процессуального кодексов и Законов Украины «Про Национальную полицию», «Про оперативно-розыскную деятельность», актуальной является задача существенного улучшения деятельности правоохранительных органов по предотвращению и выявлению указанной категории преступлений, а также их эффективному досудебному расследованию.

Состояние исследования. Научный анализ выявления и предотвращения мошенничеств через сеть Интернет, а также взаимодействия оперативных подразделений Национальной полиции Украины во время досудебного расследования с другими подразделениями был предметом исследований в области криминального процесса, криминалистики и оперативно-розыскной деятельности таких ученых, как В.М. Бутузов, И.О. Воронов, В.Д. Гавловский, Е.О. Дидоренко, М.В. Емельянов, И.П. Козаченко, Я.Ю. Кондратьев, О.Ф. Долженков, О.М. Бандурка, О.М. Джужа, А.П. Закалюк, О.Г. Кулик, Д.О. Максимус, П.П. Михайленко, О.В. Межевой, О.И. Хараберюш, Д.В. Безруков, А.М. Бабенко, С.В. Самойлов, М.В. Стащак, К.В. Титунина, В.П. Шеломенцев, О.О. Юхно.

Целью и задачей статьи является исследование, которое заключается в разработке теоретических основ и научно обоснованных практических рекомендаций по выявлению, предотвращению и досудебному расследованию мошенничеств, совершаемых с использованием сети Интернет. Для достижения поставленной цели необходимо решить такие задачи, как определение способов совершения мошенничеств в сети Интернет, характеристика выявления и предотвращения мошенничеств через сеть Интернет с помощью оперативных подразделений НПУ, исследование особенностей взаимодействия оперативных подразделений НПУ во время досудебного расследования этих преступлений и взаимодействия с другими подразделениями.

Изложение основного материала. Современное состояние общественной жизни в Украине на фоне последствий всемирного экономического кризиса характеризуется нестабильностью в экономической и политической сферах, резким социальным и материальным расслоением населения, значительными качественными изменениями в структуре преступности. Стремительное развитие использования сети Интернет в качестве поставщика товара и различных услуг, соответственно, сферы денежного обращения привело к тому, что все большее количество населения Украины становится жертвами мошенничеств, совершаемых с использованием сети Интернет.

С начала XXI века Интернет окончательно закрепил за собой статус неотъемлемой части жизнедеятельности человечества. Примерно в это время начинает появляться большое количество социальных сетей, торговых площадок и других «организаций», которые предоставляют услуги в различных сферах жизнедеятельности. Обозначенные нововведения быстро набирают популярность, что в первую очередь связано с тем, что Интернет предлагает значительно более низкую цену, чем привычные торговые места, большее количество услуг и более широкий ассортимент, включая редкие и запрещенные для свободной продажи товары. К тому же все это для удобства в основном сконцентрировано на одном интернет-ресурсе.

В то же время Интернет предоставляет возможность осуществления расчетов за полученные услуги и товары электронными платежками. К сожалению, не всегда эти технологии используются на благо. В наши дни существует огромное количество приемов и хитростей, придуманных для того, чтобы путем обмана, то есть мошенничества, завладеть имуществом других лиц. В частности, благодаря тому, что Интернет является практически неподконтрольной правоохранительным органам сферой жизнедеятельности человечества, он притягивает к себе внимание преступной среды, которая, манипулируя человеческими чувствами (от помощи, благотворительности ближнему, армии, государству до банального чувства жадности, желания максимально сэкономить, получить бесплатные подарки и т. п), пытается завладеть чужой собственностью, денежными средствами и другими материальными и нематериальными объектами, опираясь на возможности Интернета и стараясь избежать ответственности, поскольку общение и договоренности происходят в виртуальном пространстве. Сегодня даже приблизительное количество способов подготовки и совершения мошенничества с помощью Интернета невозможно четко определить, поскольку каждый день преступники придумывают новые.

По этому поводу следует привести мнение американского исследователя Дэвида Пога, который выделил больше всего видов мошенничества в Интернете. В частности, он отмечает, что большинство пользователей знает способы «сравнительно честного отъема денег», однако миллионы людей ежегодно страдают от указанного вида преступности. Д. Пог пришел к простому выводу о том, что самые действенные виды мошенничества строятся по одному и тому же принципу: начинаются с очень интересного предложения по приобретению чего-либо или предоставления услуг (чаще всего предлагается получить бесплатно то, что стоит значительных денег), впоследствии предполагают получение наперед за это денежных средств, после чего мошенники пропадают из поля зрения потерпевшего [1].

Итак, к популярным видам мошенничества Д. Пог отнес следующие:

1) «нигерийские письма счастья» (так называемые сообщения о том, что где-то далеко умер родственник и оставил наследство пострадавшему, для получения которого необходимо перечислить денежные средства в целях решения всех формальных вопросов);

2) онлайн-продажа (мошенник, притворяясь покупателем, пишет продавцу, что готов отправить почтой чек, который покрывает и стоимость покупки, и сумму, которая необходима для пересылки; продавец действительно получает чек, оплачивает отправку товара, а потом выясняется, что чек был фальшивый, продавец лишается как товара, так и денег);

3) «идеальная девушка» (распространенный вид мошенничества на сайтах знакомств заключается в том, что «идеальный» партнер желает приехать в гости к будущему потерпевшему лицу, однако не имеет средств и занимает их у него, после чего пропадает со связи);

4) «фишинг» (мошенники присылают потенциальной жертве письмо с банка или платежной системы, например “PayPal”, в котором написано, что со счетом жертвы есть проблемы, для решения которых необходимо перейти по ссылке из письма; чаще всего это требование сопровождается угрозой блокировки банковского счета, после чего мошенники получают персональные данные, а все средства с банковских сайтов исчезают) [1];

5) поддельная банковская карта (популярный в США и Канаде вид сетевого мошенничества, в ходе которого жертва получает сообщение по электронной почте с предложением получить кредитную карту с большим лимитом и чрезвычайно низкой процентной ставкой; все, что требуется от жертвы, – это внести небольшую абонентскую плату);

6) помощь друзьям, знакомым или другим лицам (самая популярная схема, которая может применяться с использованием самых разных методов коммуникации: электронной почты, социальных сетей, мессенджеров; потерпевшее лицо получает сообщение от друга или даже родственника, в котором содержится описание какой-то неприятности, которая случилась с ним/ней; в любом случае срочно нужны деньги, которые необходимо выслать на определенный счет);

7) работа на дому (мошенники предлагают жертвам высокооплачиваемую работу на дому, однако соискателю нужно сначала что-то купить, например клей для марок, какое-то оборудование, или же оплатить хостинг для веб-сайта);

8) поддельный вирус (потерпевшее лицо посещает какой-то сайт в Интернете, внезапно выскакивает окошко с предупреждением «Ваш компьютер заражен!», далее жертве предлагают пройти по ссылке для сканирования компьютера и очистки от вирусов за уплату определенной суммы денег) [2].

Однако наиболее распространенными видами мошенничества в Украине являются такие:

1) организация добровольческих, благотворительных взносов, в частности, для больных детей и бойцов АТО;

2) использование электронных торговых площадок, в частности “HIFI FORUM”, “OLX”;

3) распространение по акции или по заниженной цене любых товаров или вещей;

4) продажа или предложение доставки по низкой цене автомобилей на иностранной регистрации или под заказ у «серых» автодилеров;

5) распространение «фишинговых» программ и вирусного программного обеспечения;

6) продажа товаров в группах, которые функционируют в социальных сетях [2];

7) социальный инжиниринг (метод проникновения в защищенные системы, основанный на использовании социальной психологии), который используется с применением компьютера или телефона для доступа к счету или облегчения такого доступа, или получения ценной информации (адрес электронной почты лица) для целенаправленной кражи персональных данных [3, с. 9];

8) предложение явно несуществующей услуги или методики (генератора электронных средств, пополнение так называемых кошельков с электронными деньгами, ставки на спорт);

9) рассылка разного рода электронных писем на электронные почтовые ящики, текст которых вводит в заблуждение получателя, акцентирует внимание последнего на необходимости осуществления определенного рода платежей [3, с. 11].

Приоритетным направлением противодействия мошенничеству в сети Интернет, в том числе оперативно-розыскного противодействия, является предотвращение этих преступлений (профилактика, предупреждение и прекращение), что предусматривает такие формы, которые призваны сдержать лицо от намерения совершить преступление или доказать преступный умысел до конца. Противодействие мошенничеству в сети Интернет оперативно-розыскными мероприятиями включает систему оперативно-розыскных и других мероприятий и реализуется в отдельных организационно-тактических формах.

Предупреждение преступлений является комплексной деятельностью. Предотвращение преступлений – это сложный процесс, а его содержание отличается от других видов деятельности. При этом выделяют ряд составляющих, таких как профилактика, предотвращение и пресечение преступлений. Каждый из этих элементов самостоятелен, но они взаимосвязаны, имеют одну и ту же цель, заключающуюся в недопущении совершения преступления. Как правильно отмечает А.П. Закалюк, термин «предотвращение преступлений» обычно употребляют в отношении определенной угрозы, которая уже существует. Предотвращение означает деятельность, препятствующую совершению преступлений. Цель меры пресечения заключается в том, чтобы помешать совершению преступлений, сократить их деятельность, уменьшить размеры преступности [4, с. 318]. Под предотвращением понимается деятельность, направленная на недопущение преступлений, которые замышляются или готовятся, а под прекращением – действия, обеспечивающие прекращение уже начатых преступлений на стадии покушения либо последующих эпизодов при длящихся или так называемых серийных преступлениях [4, с. 121]. В литературе под предупреждением преступлений чаще всего понимается деятельность субъектов и участников профилактики:

– по выявлению, нейтрализации или устранению причин преступности

и отдельных ее видов, а также условий, способствующих совершению преступлений (общая профилактика);

– по выявлению, осуществлению профилактического действия и воздержанию от повторного совершения преступлений лицами, частные особенности которых указывают на реальную возможность перехода на преступный путь, а также осуществлению профилактических действий на их ближайшее окружение с целью положительной корректировки этих лиц (индивидуальная профилактика) [5, с. 253].

Пресечение преступлений имеет место, когда процесс совершения преступления останавливается внешним воздействием на стадии приготовления или покушения, когда преступник только подготавливает средства или орудия совершения преступления, ищет соучастников, осуществляет сговор на совершение преступления, либо когда процесс преступного посягательства пресекается до того, как была достигнута его цель, причинен преступный вред.

Глобальность современных возможностей и достижений человечества прямо пропорциональна глобальности угроз и преступных проявлений. В то же время развитие интернет-технологий позволило поднять на новый интернационально-континентальный уровень торгово-экономические отношения и электронную коммерцию. Изменились, укрепившись, и позиции транснациональной преступности, которые приобрели новые черты и неограниченные возможности [6, с. 63]. В последнее время широкого распространения и популяризации получило использование децентрализованных виртуальных криптовалют, таких как Bitcoin (BTC), Litecoin (LTC), Namecoin, Zerocoin, Quark, Megacoin, Namecoin, Peercoin, Worldcoin. Темпы прироста капитала их владельцев составляли в отдельные дни 100%, 200% и даже 1 000%. Криптовалюта стала одним из видов электронных платежных средств для оплаты товаров и услуг в сети Интернет, кроме того, ее можно обменять на реальные деньги.

Точных данных по количеству пользователей BTC не установлено, однако курс этой валюты с 2011 года вырос более чем в 200 раз, сделав многих ее держателей миллионерами. Сложность отслеживания платежных операций, отсутствие платы за транзакции, отсутствие необходимости предоставления идентифицирующих или разрешительных документов, большая скорость расчетов способствуют стремительному увеличению спроса, а с ним и котировочного курса. Сегодня сотни компаний мира рассчитываются криптовалютой, покупая товары и оплачивая услуги. Так, во время игры в казино в г. Лас-Вегасе (США) принимают ставки в BTC. До недавнего времени дорожал только BTC, который называют «электронным золотом», и LTC, именуемый «электронным серебром». Однако когда в конце прошлого года курс одного BTC вырос до 1 000 долл., то на рынке криптовалют возник беспрецедентный ажиотаж. Люди начали вкладывать деньги во все криптовалюты подряд, даже неликвидные. Благодаря этому возросла стоимость ближайших конкурентов BTC, которыми можно торговать на электронной бирже. Нерегулируемая сфера обращения виртуальных валют стала пользоваться большой популярностью среди организованных преступных группировок, которые принимают оплату за свои услуги в виртуальной валюте, используя альтернативный «темный» Интернет (DarkNet), функционирующий на основе системы “The Onion Router” (TOR).

Мошенничество с криптовалютами является серьезной проблемой для такой развитой страны как США, банковские регуляторы которой обратили внимание на рост количества указанных преступлений. Управление финансовых услуг г. Нью-Йорка, установив, что нерегулируемая сфера виртуальных валют пользуется большой популярностью среди интернет-мошенников, пришло к выводу, что этот вид мошенничества угрожает национальной безопасности США. Также в некоторых странах, в частности Китае, Таиланде, операции с BTC являются незаконными. Так, Национальный банк Китая запретил кредитно-финансовым учреждениям государства любые операции, связанные с BTC, пытаясь избежать рисков для отечественной экономики. Необходимо отметить, что запрет касается только юридических лиц, а граждане могут вкладывать свои сбережения на собственное усмотрение. Итак, криптовалютная торговля превратилась в глобальную азартную игру, в которую легко включиться, ведь достаточно просто купить виртуальные деньги на бирже, то есть виртуальные валюты – это огромные мировые мошеннические пирамиды.

Резкий рост популярности криптовалют заставил многих украинцев тоже задуматься над тем, чтобы осуществлять такие расчеты, а также зарабатывать на майнинге, то есть добычи BTC. Общий порядок проведения перевода средств в границах Украины, ответственность субъектов перевода средств, а также правовые требования к осуществлению выпуска и использованию электронных денег в Украине установлены Законом Украины «О платежных системах и переводах средств в Украине». Согласно статьям 9 и 15 этого Закона платежные организации платежных систем, участники платежных систем и операторы услуг платежной инфраструктуры имеют право осуществлять деятельность в Украине исключительно после их регистрации Национальным банком Украины (НБУ), который также имеет исключительное право выпуска электронных денег. Сегодня в НБУ не обращались банки или другие юридические лица по поводу регистрации платежной системы BTC или согласования правил использования электронных денег BTC. НБУ предостерегает украинцев от использования такой системы, то есть в Украине жесткой реакции со стороны органов власти и управления по операциям с криптовалютами пока не было. По нашему мнению, это связано с недооценкой уровня возможного негативного влияния криптовалюты на экономику, состояния преступности и функционирования кредитно-банковской системы государства.

Обязательными признаками объективной стороны мошенничества является общественно опасное деяние и способ совершения преступления. Сущностью деяния является завладение предметом посягательства или получение права на него. Способами совершения мошенничества являются обман и злоупотребление доверием. При совершении мошенничества обман или злоупотребление доверием предшествует моменту перехода предмета преступления во владение

виновного, а также обусловливает этот переход. При этом потерпевший (собственник или другое лицо), будучи введенным в заблуждение, или сам передает эти предметы либо права на них, или дает согласие на их получение. Однако это не исключает случаев мошеннического завладения определенными предметами или правом на них (особенно недвижимостью) и без участия потерпевшего, то есть лишь за счет использования всевозможных подделок, фальсификаций и коррупционных схем. Мошенничество считается оконченным преступлением, если виновный завладевает предметом преступления исключительно при помощи обмана или злоупотребления доверием, после чего имеет реальную возможность распорядиться им, как своим [7, с. 175].

С введением в действие нового УПК Украины в 2012 году, кроме прочего, предстали вопросы обеспечения законности при проведении оперативными подразделениями НСРД во время досудебного расследования мошенничества. Для решения этих проблем необходимо понимать сущность негласных следственных (розыскных) действий и содержания обеспечения законности при их проведении уполномоченными оперативными подразделениями.

Негласные следственные (розыскные) действия УПК Украины определяет как разновидность следственных (розыскных) действий, сведения о факте и методы проведения которых не подлежат разглашению, за исключением случаев, предусмотренных в Кодексе (часть 1 статьи 246). Законодатель установил исчерпывающий перечень таких действий. В частности, к ним отнесены аудио-, видеоконтроль лица (статья 260); наложение ареста на корреспонденцию (статья 261); осмотр и выемка корреспонденции (статья 262); снятие информации с транспортных телекоммуникационных сетей (статья 263); снятие информации с электронных информационных систем (статья 264); обследование публично недоступных мест, жилья или иного владения лица (статья 267); установление местонахождения радиоэлектронного средства (статья 268); наблюдение за лицом, вещью или местом (статья 259); аудио-, видеоконтроль места (статья 270); контроль над совершением преступления (статья 271); выполнение специального задания по раскрытию преступной деятельности организованной группы или преступной организации (статья 272); негласное получение образцов, необходимых для сравнительного исследования (статья 274); использование конфиденциального сотрудничества (статья 275) [8].

Согласно части 6 статьи 246 УПК Украины НСРД по поручению следователя могут осуществлять уполномоченные оперативные подразделения. Полномочия следователя поручать такие действия соответствующим оперативным подразделениям установлены пунктом 3 части 2 статьи 40, а обязанность их выполнения возложена на эти подразделения частью 3 статьи 41 указанного Кодекса. Эти положения вполне логичны, поскольку следователи для личного проведения НСРД сегодня не имеют ни средств, ни времени, ни профессиональных навыков. Ученые признают законность основным принципом ОРД. Ее рассматривают как фундаментальное положение, обуславливающее существование и пронизывающее всю систему принципов этой деятельности. Принцип законности удостоверяет неразрывную связь ОРД с правом.

С.Д. Гусарев, Р.А. Калюжный, А.М. Колодий, А.Ю. Олейник, О.Л. Слюсаренко, О.В. Шмоткин отмечали, что законность – это явление многогранное, которое может рассматриваться как принцип формирования правового государства, как метод управления обществом, как режим точного выполнения закона. Законность также трактуют как совокупность требований и гарантий, обеспечивающих порядок в государстве [9, с. 42]. Следует согласиться с Э.А. Дидоренком, И.П. Козаченком, Я.Ю. Кондратьевым, В.П. Пилипчуком, В.Л. Регульським в том, что соблюдение принципа законности в ОРД сводится к исполнению, в частности, таких требований:

– ОРД осуществляют только определенные в законе подразделения;

– ОРМ запрещаются при отсутствии оснований, предусмотренных законом;

– исключительные и временные меры, ограничивающие права и свободы человека, употребляют только тогда, когда другим способом невозможно добыть фактические данные для обеспечения интересов уголовного судопроизводства;

– в случае нарушения прав и свобод человека или юридических лиц, а также если причастность к правонарушению объектов ОРМ не подтвердилась, то оперативные подразделения должны восстановить нарушенные права и возместить причиненные материальные и моральные убытки;

– граждане имеют право в установленном законом порядке получить от органов, в компетенцию которых входит ОРД, письменное объяснение по поводу ограничения их прав и свобод, а также обжаловать эти действия;

– конфиденциальное сотрудничество с лицами должно устанавливаться только на основе добровольности;

– опрос граждан, посещение жилых и других помещений, использование их и транспортных средств в оперативно-розыскных целях должны осуществляться с согласия граждан или администрации предприятий, учреждений, организаций (за исключением негласных мероприятий);

– лица, осуществляющие ОРД, и те, которых привлекают к выполнению ее задач, находятся под защитой государства [9, с. 61].

Из анализа указанных положений в плоскости проведения оперативными подразделениями НСРД во время досудебного расследования мошенничества следует вывод, что большинство приведенных требований их не касаются, ведь эти подразделения не имеют права принимать самостоятельные решения о проведении НСРД и действуют по поручениям следователей. Именно следователи определяют, есть ли возможность получить необходимую информацию без привлечения сил и средств оперативных подразделений.

Собственно, они и будут отвечать за нарушение прав, свобод граждан и возмещать убытки лицам, которые неоправданно стали объектами НСРД. Непосредственно инициатор (следователь, прокурор) должен давать объяснения по поводу ограничения прав и свобод граждан в случае их обращения о незаконном проведении в отношении указанных касательно них НСРД. Все это обусловливает необходимость исследования принципа законности

в деятельности оперативных подразделений на уровне конкретных НСРД, проводимых во время досудебного расследования мошенничества. Такое исследование целесообразно основывать на результатах научного поиска проблем законности ОРЗ.

Комментируя указанные положения в контексте работы оперативных подразделений по исполнению поручений на проведение НСРД во время досудебного расследования мошенничества, можем прийти к таким выводам:

– использование оперативно-розыскных возможностей только в пределах своей компетенции соответствует проведению НСРД только по поручениям следователя (прокурора), оформленным в установленном порядке (субъектами исполнения таких поручений могут быть оперативные подразделения, в компетенцию которых входит противодействие мошенничеству, а также оперативные подразделения, которые специализируются на проведении отдельных НСРД);

– требование невозможности проведения мероприятий в отношении лиц, не причастных к преступной деятельности, не может в полной мере (по вполне объективным причинам) быть внедрено в практику оперативных подразделений по исполнению поручений на НСРД при досудебном расследовании преступлений мошенничества, ведь круг подозреваемых в совершении мошенничества иногда оказывается достаточно широким, а НСРД являются одними из средств, которые позволяют его сузить, поэтому поручение на их проведение часто оформляют в отношении нескольких подозреваемых.

Следует отметить, что определенная часть объектов НСРД, в конце концов, оказывается непричастной к преступной деятельности, но нарушения законности здесь нет. Вынужденное вмешательство в личную жизнь граждан в таких случаях осуществляют исключительно с целью расследования тяжких и особо тяжких преступлений. Хотя эти лица не причастны к преступной деятельности, проведение в отношении них НСРД происходит в рамках отработки следственных версий во время досудебного расследования мошенничества, а в итоге способствует разоблачению настоящих преступников. Законность нарушается в том случае, когда в уголовном производстве, на основе которого оформлено задание на НСРД, отсутствуют данные, указывающие на вероятность причастности объектов к совершению или приготовлению конкретного мошенничества. Такое нарушение законности происходит по вине инициатора (следователя, прокурора), который ведет уголовное производство. Сотрудников оперативного подразделения можно считать виновными в нарушении законности, если они осуществляют мероприятия без оформления поручения или задания. Такое случается тогда, когда силы и средства оперативных подразделений используют не по назначению (без цели борьбы с преступностью).

Бесспорно, НСРД, как и ОРМ, должны обеспечивать своевременное выявление, раскрытие и расследование мошенничества в кратчайший срок. Однако это, вероятнее всего, касается вопросов эффективности ОРД и уголовного процесса, а не обеспечения их законности.

Выводы. Мошенничество, совершенное с использованием сети Интернет, является специфическим явлением в современной преступности, поскольку может как иметь проявления внутри государства, так и охватывать территории других государств, приобретая транснациональный характер. Установлено, что анализируемому виду мошенничества присущи одновременно и обман, и злоупотребление доверием. На основе изложенного выше с целью предотвращения и нейтрализации реальных и потенциальных угроз национальной безопасности Украины, противодействия деструктивному влиянию виртуальных валют на развитие экономики Украины, предотвращения их использования для совершения преступлений в сети Интернет вообще и мошенничества в частности считаем целесообразным осуществить следующие мероприятия: принять меры по ограничению в Украине операций с использованием криптовалют; по результатам деятельности экспертов межведомственной рабочей группы рассмотреть вопрос о наработке соответствующих изменений и дополнений законодательства Украины касательно регулирования вопросов, связанных с операциями с криптовалютами в Украине; наладить международное сотрудничество с государствами, имеющими соответствующий опыт противодействия деструктивному влиянию криптовалюты.

Список использованной литературы:

1. Самойлов С.В. «Фишинг» как способ совершения интернет-мошенничеств. *Актуальные вопросы современных государственных и правотворческих процессов* : материалы международной научно-практической конференции (г. Запорожье, 24 февраля 2011 года). Запорожье : Запорожская городская общественная организация «Истина», 2011.

2. Бросалы-онлайн. Названы самые распространенные способы интернет-мошенничества. *Новое время*. URL: http://nv.ua/techno/gadgets/kidaly-onlajn-nazvany-samye-rasprostranennye-sposobyinternet moshennichestva-75741.html (дата обращения: 22.10.2017).

3. Телійчук В.Г., Санакоєв Д.Б., Ковч Я.М., Козорог О.В. Алгоритм дій працівників підрозділів карного розшуку під час розкриття шахрайств, вчинених через мережу Інтернет: методичні рекомендації. Дніпро : Дніпропетровський державний університет внутрішніх справ, 2018. 55 с.

4. Закалюк А.П. Курс современной украинской криминологии: теория и практика : в 3 кн. Кн. 1 : Теоретические основы и история украинской криминологической науки. Киев : Ин-Юре, 2007. 424 с.

5. Джужа О.М., Кондратьев Я.Ю., Кулик О.Г., Михайленко П.П. и др. Криминология : учебник для студентов высших учебных заведений. Киев : Юринком-Интер, 2002. 416 с.

6. Shapochka S. Preventing Fraud Using Computer Networks. *Internal Security*. 2013. № 2. P. 63–75.

7. Емельянов М.В. Уголовно-правовая характеристика мошенничества : дисс. … канд. юрид. наук : спец. 12.00.08. ; Харьковский национальный университет внутренних дел. Харьков, 2013. 336 с.

8. Уголовно-процессуальный кодекс Украины от 13 апреля 2012 года № 4651-VI. *Відомості Верховної Ради*

Україні. 2013. № 9–10, № 11–12, № 13. С. 88.

9. Гусарев С.Д., Калюжный Р.А., Колодий А.М. и др. Основы государства и права : учебное пособие. Киев : Лыбидь, 1997. 209 с.

ИНФОРМАЦИЯ ОБ АВТОРАХ

Телийчук Виталий Григорьевич – кандидат юридических наук, старший научный сотрудник, доцент, доцент кафедры оперативно-розыскной деятельности факультета подготовки специалистов для подразделений криминальной полиции Днепропетровского государственного университета внутренних дел;

Горелик Дарья Сергеевна – соискатель высшего образования факультета подготовки специалистов для подразделений криминальной полиции Днепропетровского государственного университета внутренних дел

INFORMATION ABOUT THE AUTHOR

Teliychuk Vitaliy Grigoryevich – Candidate of Law Sciences, Senior Researcher, Associate Professor, Associate Professor at the Department of Operatively-Search Activity of Faculty of Preparation of Experts for Subdivisions of Criminal Police of Dnepropetrovsk State University of Internal Affairs;

Gorelik Daria Sergeyevna – Applicant for Higher Education of Faculty of Training Specialists for Criminal Police Units of the Dnepropetrovsk State University of Internal Affairs

Vikol_grigor@ukr.net

УДК 342.729

АДМИНИСТРАТИВНО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ПРАВА НА МИРНЫЕ СОБРАНИЯ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Ольга ТИЛИПСКАЯ,
аспирант кафедры административного права
Киевского национального университета имени Тараса Шевченко

АННОТАЦИЯ

В статье проведено теоретическое исследование основ административно-правового обеспечения права на мирные собрания в Российской Федерации, а именно изучение и анализ правовой основы реализации и обеспечения права на мирные собрания, уровня соблюдения права на мирные собрания в Российской Федерации. Приведены статистика, основания и суть нарушений права на мирные собрания судами и другими органами права на мирные собрания в России. Продемонстрирована эволюция ужесточения законодательства РФ в сфере мирных собраний, приведены практические примеры кричащего нарушения права на мирные собрания в России и на оккупированных территориях.

Ключевые слова: мирные собрания, ограничение права, Российская Федерация, обеспечения права, право на мирные собрания, специальный закон.

ADMINISTRATIVE AND LEGAL GUARANTEE OF THE RIGHT TO PEACEFUL ASSEMBLY IN UKRAINE

Olga TILIPSKAYA,
Postgraduate Student at the Department of Administrative Law
of Taras Shevchenko National University of Kyiv

SUMMARY

In the article the theoretical research is providing the foundations of the administrative and legal support of the right to peaceful assembly in the Russian Federation, namely, the study and analysis of the legal basis for the exercising and enforcement of the right to peaceful assembly, the level of compliance with the right to peaceful assembly in the Russian Federation. The article provides statistics, grounds and essence of violations of the right to peaceful assembly by courts and other bodies of the right to peaceful assembly in Russia. The evolution of toughening of the legislation of the Russian Federation in the field of peaceful assembly is demonstrated and flashy practical examples of violation of the right to peaceful assembly in Russia and in the occupied territories is given.

Key words: peaceful assembly, restriction of right, Russian Federation, guarantee the right, right to peaceful assembly, special law.

Постановка проблемы. Показателями уровня демократии в государстве, как известно, являются реальное представительное народовластие и реальное обеспечение прав и свобод человека и гражданина, уважение к ним. Особое значение среди последних обычно занимают политические права и свободы.

В последние годы в Украине и Российской Федерации возросли активность и самосознание населения, что получило выражение в демонстрациях, пикетах, автопробегах и других формах мирных собраний. Однако в Украине, в отличие от практики РФ, массовые мирные собрания, как правило, достигают поставленных целей и уже не раз доказывали свою эффективность в разрезе влияния на жизнь государства. В связи с тем, что право на мирные собрания является одним из столпов демократии по требованию европейских стандартов по правам человека, необходимо изучать негативную практику обеспечения права на мирные собрания в Российской Федерации.

Актуальность темы исследования подтверждается тем, что для обогащения доктрины права в Украине, совершенствования законодательства в сфере мирных собраний и становления устоявшейся судебной практики в рамках утверждения презумпции правомерности мирных собраний и уважения к корреспондирующему праву необходимо изучать и негативный опыт таких