следует рассматривать как веса на ребрах графа. Соответственно, каждое входящее ребро в транзакции несет метку времени и количество биткоинов, формирующих вход для указанных транзакций;

метод построения и анализа графа адресов. Его сущность сходна с приведенным выше. Анализируя граф транзакций G, исследователь может выявить корреляцию между различными входными и выходными адресами. Открытые ключи и соответствующие взаимосвязи можно использовать для построения графа адресов G = {P, E}, где P – это набор биткоин-адресов, а E – ребра, соединяющие эти адреса.

метод построения и анализа графа пользователя. Предполагает создание на основе вышеприведенных эвристических подходов графа пользователя путем группировки адресов, которые предположительно принадлежат одному и тому же владельцу.

Каждый из вышеприведенных методов деанонимизации состоит из двух этапов: этапа сбора данных и этапа анализа данных. Сбор данных может осуществляться как в режиме онлайн (например, с применением специально разработанных обфусцированных биткоин-узлов, содержащих модифицированное программное обеспечение, позволяющее перехватывать трафик, исследовать механизм распространения адресов, устанавливать прямую связь с другими узлами в сети), так и в автономном режиме с использованием обычного биткоин-кошелька.

Изложенное является лишь частным фрагментом важной проблемы выявления и пресечения преступлений, совершаемых с использованием криптовалют. В сочетании с соответствующими оперативно-розыскными подходами представленные в работе методы деанонимизации публичных биткоин-адресов могут помочь сотруднику органов внутренних дел установить лицо, совершившее преступление рассматриваемого вида.

Список использованных источников

1. Перов, В.А. Выявление, квалификация и организация расследования преступлений, совершаемых с использованием криптовалюты : учеб.-метод. пособие / В.А. Перов. – М. : Юрлитинформ. – 2017. – 200 с.

2. Сидоренко, Э.Л. Криминологические риски оборота криптовалюты и проблемы ее правовой идентификации / Э.Л. Сидоренко // Б-ка криминалиста. Науч. журн. – 2016. – № 3 (32). – С. 148–154.

3. Батоев, В.Б. Использование криптовалюты в преступной деятельности: проблемы противодействия / В.Б. Батоев, В.В. Семенчук // Тр. Акад. упр. МВД России. – 2017. – № 2. – С. 9–15.

4. Авдошин, С.М. Методы деанонимизации пользователей Bitcoon / С.М. Авдошин, А.В. Лазаренко // Тр. ИСП РАН. – Вып. 30. – 2018. – С. 89–102.

5. Накамото, С. Биткоин: одноранговая электронная кассовая система [Электронный ресурс] / С. Накамото // Биткоин [Офиц. сайт]. – Режим доступа: https://bitcoin.org/bitcoin.pdf. – Дата доступа: 22.10.2022.

6. Андрукли, Э. Оценка конфиденциальности пользователей в биткоинах [Электронный ресурс] / Э. Андрукли, Г.О. Караме // Cryptology ePrint Archive [Офиц. сайт]. – Режим доступа: https://eprint.iacr.org/2012/596.pdf. – Дата доступа: 22.10.2022.

7. Голдфедер, С. Когда cookie встречается с блокчейном: риски конфиденциальности веб-платежей через криптовалюты [Электронный ресурс] / С. Голдфедер // Б-ка Корнел. ун-та [Офиц. сайт]. – Режим доступа: https://arxiv. org/pdf/708.04748.pdf. – Дата доступа: 22.10.2022.

УДК 34:004.77

П.Л. Боровик

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В УСЛОВИЯХ ГЛОБАЛИЗАЦИИ ИНФОРМАЦИОННОГО ПРОСТРАНСТВА: АКТУАЛЬНЫЕ ПРОБЛЕМЫ И ПУТИ ИХ РЕШЕНИЯ

Актуальность проблемы информационной безопасности обусловлена фундаментальной зависимостью всех сфер современного социума (экономика, культура, наука, медицина, правоохранительная деятельность и др.) от нормального развития и обмена информацией, что связано с повсеместным внедрением новейших информационно-коммуникационных технологий (ИКТ). Данное утверждение аргументируется рядом обстоятельств:

в условиях глобализации информационного пространства реализация жизненно важных интересов личности, общества и государства осуществляется посредством процессов информатизации, т. е. указанные субъекты видят реализацию своих интересов через призму получения благ, предлагаемых развитием информационных отношений, и желают развиваться в данном направлении;

в контексте всеобщей цифровизации информационная сфера приобрела статус системообразующей, и от нее в значительной степени зависит уровень экономического, социального, политического развития общества и государства;

специфика информационной среды такова, что негативные последствия реализации угроз информационной безопасности проявляются в других сферах жизнедеятельности личности, общества и государства и влияют на национальную безопасность в политической, экономической и иных областях;

анализ существующих в мире вызовов и угроз показывает, что в современных условиях возрастает опасность совершения трансграничных преступлений, возникновения кризисных ситуаций и иных противоправных действий с применением современных ИКТ.

В таких условиях особую актуальность приобретают вопросы формирования активной согласованной информационной политики международного сообщества и развития единого информационного пространства, создания совместного потенциала по противодействию информационным угрозам и обеспечению информационной безопасности, защиты информационных ресурсов и коммуникаций национальных органов власти и управления.

Отдельные аспекты данной проблемы в различные периоды исследовались в научных работах Э.Л. Бернейса, Н.А. Брусницына, Г.В. Вирена, В.Б. Вепринцева, Л. Войтасика, Д.А. Волкогонова, А.Б. Губарева, Л.В. Воронцовой, В.К. Новикова, И.Н. Панарина, Г.Г. Почепцова, С.П. Расторгуева, Д.Б. Фролова и др. Несмотря на пристальное внимание ученых и специалистов к этому вопросу, как в нашей стране, так и за рубежом, в настоящее время не существует единого терминологического аппарата и согласованного подхода к реализации политики международной информационной безопасности, а нормативная база, регулирующая методы и технологии ведения и противодействия кибервойнам, требует глубокого изучения и политологической концептуализации. В связи с этим обеспечение информационной безопасности становится одной из важнейших задач современного политического управления на государственном уровне с целью сохранения суверенитета национального пространства политических коммуникаций, включая национальные сегменты сети Интернет.

Следует отметить, что концептуальные методологические подходы к обеспечению информационной безопасности непосредственным образом опираются на государственные и международные нормативные правовые акты, регулирующие внутренние и внешние политические отношения. Ключевую роль при этом играют национальные стратегии информационной безопасности (кибербезопасности) – концептуальные документы, принятые в том или ином государстве, в соответствии с которыми осуществляется политика обеспечения информационной безопасности страны.

Изучение действующих стратегий информационной безопасности иностранных государств (США, Швеция, Эстония, Словакия, Финляндия, Голландия, Чехия, Литва, Германия, Франция и др.) показало, что их концептуальные подходы основываются на принципах, закрепленных в ключевых документах, к важнейшим из которых относятся стратегии информационной безопасности или равнозначные им по своим

функциям документы. Информационная безопасность рассматривается как стратегическая проблема государственной важности, затрагивающая все слои общества. Участие ряда стран, в частности, членов ЕС в общей оборонной организации НАТО, во многом определяющей конкретные методы обеспечения информационной безопасности, также способствует сходству политических курсов отдельных европейских стран в сфере информационной безопасности.

Вместе с тем результаты анализа содержания вышеприведенных стратегий свидетельствуют о том, что как на европейском, так и на международном уровне отсутствуют единые подходы к пониманию категории «информационная безопасность» («кибербезопасность») и других ключевых терминов. Как следствие, различаются и подходы к составлению стратегий, что приводит к невозможности сформулировать общие цели для международного сообщества по обеспечению информационной безопасности на глобальном уровне. Отсутствие общего «языка» и согласованного подхода усложняет процесс международного сотрудничества в данной сфере, ведь важность сотрудничества признается всеми странами. Кроме того, отсутствие конкретных планов действий в принятых стратегиях, отчетливого указания их целей, а также спектра решаемых проблем приводит к невозможности сформулировать конкретные практические рекомендации по реализации поставленных целей и задач для правительственных ведомств, национальных органов власти и других государственных органов.

Таким образом, проблема информационной безопасности в условиях глобализации носит комплексный, международный характер. Для ее решения каждое государство принимает концептуальные политические документы, к важнейшим из которых относится стратегия информационной безопасности или равнозначный ей по своим функциям документ (концепция, доктрина). Подобного рода документы не только определяют стратегические цели, конкретную политику и регулирующие меры для достижения и поддержания высокого уровня сетевой и информационной безопасности, но и играют ключевую методологическую роль в системе обеспечения национальной безопасности.

Особую актуальность приобретают вопросы формирования активной согласованной информационной политики международного сообщества и развития единого информационного пространства, создания совместного потенциала по противодействию информационным угрозам и обеспечению информационной безопасности, защиты информационных ресурсов и коммуникаций национальных органов власти и управления.

Для эффективной подготовки и своевременного реагирования на угрозы информационной безопасности необходимо согласованное ме-

ждународное сотрудничество. Первым шагом на пути к реализации этой задачи может стать принятие комплексной международной стратегии кибербезопасности. Для ее реализации необходимы:

унификация терминологического аппарата;

гармонизация законодательной базы;

разработка конкретных планов действий, отчетливое указание их целей, а также спектра решаемых проблем;

тесное сотрудничество частного и государственного сектора, осуществляемого посредством обмена информацией, передовыми практиками (например, в сфере управления инцидентами, обучения специалистов и обычных пользователей ИКТ), а также путем проведения специальных учебных мероприятий (учений, тренингов) на государственном и международном уровнях.

УДК 343.985

В.Л. Венгловский

НЕКОТОРЫЕ АСПЕКТЫ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ ПРИ ВЫЯВЛЕНИИ НАРКОПРЕСТУПЛЕНИЙ

Используя интернет-технологии наркосбытчики получили возможность продавать наркотики бесконтактным способом и в определенной степени анонимно. Посредством сети Интернет создаются интернет-магазины, осуществляется реклама, привлечение и координация действий членов преступных групп в разных регионах страны, так и за ее пределами, что потребовало от правоохранителей в целях противодействия наркопреступлениям развивать и совершенствовать информационно-аналитическую деятельность.

Проделанный анализ научной и специальной литературы показал, что среди ученых и практиков отсутствует единое понимание сущности, задач и методов информационно-аналитической деятельности, что влечет существенные проблемы не только в области теоретической проработки рассматриваемого вопроса, но и в построении эффективной правоприменительной практики, организация которой осложнена наличием большого количества субъектов, в той или иной степени решающих задачи противодействия наркопреступности.

Одной из основных проблем при создании теоретической основы данной деятельности видится необходимость определения сущности и содержания информационно-аналитической деятельности при выявлении преступлений и как ее составной части – наркопреступлений, совершаемых в сети Интернет.

Ряд авторов в своих работах используют для обозначения рассматриваемой деятельности достаточно близкие по содержанию термины: «аналитическая разведка», «аналитическая работа», «аналитическая деятельность», «аналитический поиск».

Отдельные ученые относят информационно-аналитическую деятельность к числу методов познания и понимают под ним метод, заключающийся в комплексном применении сил, средств и методов оперативно-розыскной деятельности (ОРД) по сбору, обобщению и анализу конфиденциальной и легитимной информации, обеспечивающей приращение или получение новых знаний об объектах и субъектах криминальных проявлений, для упреждающего воздействия на преступность или определяют аналитический поиск как метод ОРД, предполагающий «проникновение» в документальные источники сведений и соответствующие массивы данных, содержащих знания об объектах, представляющих оперативный интерес, и их детальное изучение в целях получения оперативно значимой информации.

Вклад в развитие информационно-аналитической деятельности внес С.С. Овчинский, который в своей монографии «Оперативно-розыскная информация» предложил концептуальные основы информационного обеспечения оперативно-розыскной и профилактической деятельности органов внутренних дел.

В работе Е.Г. Белоглазова «Методология обеспечения аналитической разведки криминальных процессов и явлений» рассмотрены виды информационно-аналитической деятельности и источники информации, основанные на информационных технологиях, также определены основные направления этой деятельности применительно к различным оперативным подразделениям органов внутренних дел.

С.В. Пилюшин в своей работе «Аналитическая деятельность в принятии управленческих решений: сущность и значение» анализирует сущность информационно-аналитической деятельности на примере деятельности по выявлению экономических преступлений. При этом автор отмечает, что аналитическая деятельность вышеуказанных сотрудников осуществляется посредством применения конкретных методов познания, где для каждого характерна совокупность определенных принципов, правил, приемов и алгоритмов, сложившихся в четкую систему в процессе их применения.

В исследовании А.С. Щуровой «Незаконный оборот наркотиков в Интернете» делается акцент на том, что особенность незаконного оборота наркотиков, совершаемого посредством сети Интернет, заключается в использовании сетей телекоммуникаций и связи. При выявлении