по ОИ, который подлежит защите. В настоящее время эта задача для объектов со сравнительно простыми функциональными связями между технологическими звеньями (элементами в звеньях) решается с использованием методов, разработанных применительно к выбору совокупности средств для воздействия по объектам противоборствующей стороны.

Основной исходной предпосылкой этих методов является предположение о полной определенности сведений относительно средств воздействия и недостаточной достоверности сведений о цели воздействия. При решении обратной задачи исходные предпосылки и в равной степени и задачи расчета коренным образом меняются. Прежде всего метод решения этой задачи должен быть чувствителен к размещению объектов на местности, их устойчивости к поражающему деструктивному воздействию, функциональным связям между элементами объекта и т. д. Отсюда следует, что основные сведения о цели должны быть известны и введены в алгоритм расчета. В то же время данные о внешнем воздействии на цель, а также ряд данных о цели (случайные отклонения от прочностных характеристик элементов цели, их ориентация относительно деструктивного воздействия и т. д.) не могут быть предсказаны точно.

Производительность объекта информатизации, определяемая оператором сопряжения последовательно-параллельной модели, будет представлять собой функцию, содержащую операции «сумма» и «выбор минимума».

При случайной вариации производительности элементов и подсистем статистические характеристики производительности объекта информатизации I = Ф(Ii) определяются методами расчета статистических характеристик функций случайных аргументов в рамках классической теории вероятностей.

Задача сводится к определению статистических характеристик вида

$$I_i = \sum_{j=1}^{m_i} I_{ij} \left(j = \overline{1, m_i} \right) \qquad (1)$$

$$I = \min_{(i)} \{ I_i \} \left(i = \overline{1, n} \right), \qquad (2)$$

где n – число технологических звеньев в системе;

m_i – число элементов, выполняющих (обеспечивающих выполнение) i -той технологической операции.

Математическое ожидание и дисперсия функций распределения «сложение» (1) и «минимум» (2) (для системы, состоящей их двух групп элементов) для случая нормального распределения определяются соотношениями, приведенным в (1).

Задача сводится к определению числовых характеристик производительностей, входящих в систему групп элементов и соответствующих корреляционных моментов.

УДК 343.8

П.Л. Боровик, В.А. Самойло

АКТУАЛЬНЫЕ МЕТОДОЛОГИЧЕСКИЕ ПОДХОДЫ К ДЕАНОНИМИЗАЦИИ ЛИЦ, СОВЕРШАЮЩИХ ПРЕСТУПЛЕНИЯ С ИСПОЛЬЗОВАНИЕМ КРИПТОВАЛЮТ

Анализ оперативно-следственной и судебной практики по делам о преступлениях, связанных с использованием криптовалют, свидетельствует, что одной из насущных проблем выявления и расследования соответствующих криминальных деяний является установление личности (идентификация) владельца публичного биткоин-адреса, с которого либо на который осуществлялась транзакция. Поскольку процесс создания криптокошелька в основном анонимен, а переводы с одного биткоин-адреса на другой не верифицируются, установить персональные сведения о лицах (IP-адрес, географическое местоположение, Ф.И.О. и пр.), участвующих в транзакции, традиционными средствами не представляется возможным.

В ходе изучения и обобщения специальной литературы, посвященной рассматриваемой проблематике [1–4], было установлено, что в основу практической деятельности по деанонимизации лиц, совершающих преступления с использованием криптовалют, может быть положен процесс привязки публичного биткоин-адреса к цифровому идентификатору пользователя или его IP-адресу. Исследование показало, что этот процесс может осуществляться с применением так называемых интерактивных, активных и пассивных методов (данное деление в некоторой степени условно, оно лишь демонстрирует степень активности субъекта оперативно-розыскной деятельности по отношению к объекту исследования).

Так, интерактивные методы деанонимизации владельца публичного биткоин-адреса могут быть реализованы с использованием социальной инженерии, позволяющей установить непосредственный контакт с владельцем с целью совершения им определенных действий или разглашения соответствующей информации. Такие методы подходят в основном для деанонимизации частично неизвестных владельцев биткоин-адресов в условной цепочке биткоин-транзакций.

В основу активных методов могут быть положены подходы, основанные на внедрении специально разработанных обфусцированных биткоин-узлов, содержащих модифицированное программное обеспечение, позволяющее перехватывать трафик либо устанавливать прямую связь с другими узлами в сети. Использование обфусцированных биткоин-узлов позволяет перехватить IP-адреса владельцев и связать с ними определенные транзакции.

Пассивные методы могут основываться на использовании данных, полученных из блокчейна (https://www.blockchain.com/) либо иного общедоступного источника информации. Применяемые при этом подходы, с одной стороны, подразумевают отсутствие прямого взаимодействия с одноранговой сетью биткоин; с другой – полагаются на комплексные и широко представленные в открытых источниках методы анализа графов и иные эвристические технологии, связанные с биткоин-протоколом.

По нашему мнению, наиболее востребованными на первоначальном этапе решения обозначенной проблемы, а следовательно, и практической значимостью, могут обладать пассивные способы, основанные на использовании эвристики – совокупности логических и аналитических приемов, методов и правил, облегчающих и упрощающих решение конкретных познавательных и практических задач.

При пассивном сборе исследователь осуществляет поиск цифровых имен пользователей публичных биткоин-адресов из открытых источников глобальной сети: веб-сайты, форумы, социальные сети, майнинговые пулы, кошельки, банковские и небанковские биржи, порталы азартных игр и др.

Пассивные методы деанонимизации владельца публичного биткоин-адреса подразделяются на следующие разновидности:

метод прямого совпадения. В его основе лежит традиционный поиск цифрового идентификатора владельца биткоин-адреса в общедоступных источниках с использованием поисковых систем;

эвристический метод нескольких входов. Основан на сопоставлении входных биткоин-адресов. Например, если сумма транзакции превышает стоимость каждого из доступных биткоинов в кошельке пользователя, то существующие биткоин-клиенты выбирают набор биткоинов из разных имеющихся адресов в кошельке владельца и выполняют платеж с помощью транзакций с несколькими входными адресами, принадлежащими одному пользователю;

анализ смены биткоин-адреса. Суть данного метода основывается на генерации в ходе транзакции сетью биткоин так называемых теневых адресов [5], на который владельцу кошелька поступает «сдача». Используя методы сопоставления и анализа, можно легко установить начальный адрес владельца кошелька, который осуществлял оплату;

метод кластеризации. Основан на двух предыдущих подходах. Используя эвристический метод нескольких входов, исследователи смогли разделить сеть на 5.579.176 кластеров пользователей, начав с 12.056.684 открытых ключей. В последующем, анализируя смену биткоин-адресов, авторы предложили новую эвристику кластеризации, основанную на изменении адреса, позволяющую выделить и объединить адреса, принадлежащие одному и тому же владельцу кошелька [6]. С помощью данного метода можно идентифицировать основные финансовые субъекты (биржи, обменники, игровые сайты и т. п.) и способы взаимодействия между ними, используя лишь незначительное количество идентифицированных транзакций;

метод анализа виртуальных следов (цифровых отпечатков). В его основе лежит механизм формирования виртуальных следов сторонними веб-трекерами в открытом сегменте сети Интернет. В литературе, посвященной рассматриваемому вопросу, отмечается, что сторонний веб-трекер в состоянии деанонимизировать пользователей криптокошельков [7]. Так, при совершении покупок в интернет-магазине и проведении соответствующих транзакций в криптовалюте в интернет-пространстве будет оставлено множество релевантных виртуальных следов. Данные следы могут быть проанализированы двумя способами:

путем сопоставления транзакции (например, если у стороннего веб-трекера имеется доступ к адресу пользователя, то привязка последнего к адресу осуществляется тривиально; в другом случае, если веб-трекер владеет информацией о стоимости (даже приблизительной) покупки и времени совершения транзакции, то исследователю достаточно получить доступ к журналу транзакций);

путем формирования кластерного перекрестка (идентификация кластера адресов, позволяющая связать две либо более покупок одних и тех же пользователей с блокчейном);

метод деанонимизации с графовым анализом, основанный на реализации алгоритмов обнаружения сообществ и метрик центральности. Для этого могут использоваться социальные сети и (или) методы социальной инженерии. Так, исследователь может выявить сообщество друзей или соседей искомого лица, найти людей в середине цепочки, замешанных в незаконной деятельности, и т. д.;

метод построения и анализа график транзакций. Его суть состоит в следующем. Всю цепочку блоков в блокчейне можно рассматривать как ациклический граф транзакций $G = \{T, E\}$, где T – множество транзакций, хранящихся в цепочке блоков, E – множество однонаправленных ребер между этими транзакциями. Указанный граф представляет собой поток биткоинов между транзакциями в блокчейне с течением времени. При этом набор входных и выходных биткоинов в транзакции

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;