полной картины о событиях, происходящих в зарубежных странах в самых различных областях, начиная с политики и заканчивая военным производством.

Особое внимание анализу открытых источников уделяется всеми структурами разведывательного сообщества. В каждом из этих органов функционируют достаточно мощные аналитически аппараты с большим количеством хорошо подготовленных специалистов. Этот вид разведки сегодня выделен в отдельную сферу деятельности спецслужб и именуется разведкой на базе анализа открытых источников информации (Open Source Intelligence – OSINT).

Традиционно защита государственных секретов рассматривается как обеспечение конфиденциальности данных сведений, однако современность создает новые угрозы информационной безопасности и ставит новые задачи в сфере защиты государственных секретов. Так, для информации, содержащейся на электронных носителях (а данный вид информации неуклонно становится доминирующим), актуализируются такие угрозы, как модификация, блокирование, уничтожение информации.

В условиях открытости информационного пространства Беларуси деструктивное воздействие на национальные объекты информационной безопасности нарушает конфиденциальность, целостность и доступность данных пользователей, права и свободы граждан, реализуются угрозы внедрения программ со встроенным вредоносным кодом, кроме того, оказывается негативное информационно-психологическое воздействие на пользователей, внедряются фиктивные ресурсы с целью получения доступа к конфиденциальным данным.

Следует отметить, что структура киберпространства является сложной и многослойной. В составе слоев этого киберпространства выделяется географическая среда, физическая инфраструктура, уровень информации, идентичность в киберпространстве, люди. Все это вносит значительные сложности в защиту государственных секретов в условиях информационной открытости.

Представляется обоснованным осуществлять классификацию методов защиты, основанную на выделении у субъекта ряда признаков, позволяющих осуществлять его идентификацию: некоторые уникальные знания; идентификаторы; биометрические характеристики, сочетание всех методов.

В реализованных на практике системах анализа рисков используют различные подходы. Приведем наиболее известные. В системе CORAS использованы качественный подход, формальная модель объекта для анализа рисков, моделирование объектов и компьютеризированные инструменты точной, однозначной и эффективной оценки рисков критически важных элементов систем безопасности. Использованы диаграммы, иллюстрирующие взаимосвязи и зависимости между пользователями и средой, в которой они работают. В системе CIRA также применен качественный подход. Но здесь выделяются заинтересованные стороны, оцениваются их действия и ожидаемые последствия в ситуации с риском. Во внимание принимается факт того, что заинтересованной стороне (владельцу стратегии защиты и владельцу риска) важен результат. В системе ISRAM оценивают вероятность проявления риска и его возможные последствия. Факторам риска присваивается значение в диапазоне от 1 до 25 ед. и в этом интервале выделяют зоны высокого, среднего или низкого риска. Полученная оценка учитывается при принятии решений. В системе IS подход многоэтапный. На первом этапе определяется относительная важность основных функций и процессов, на втором – идентифицируются активы и определяется их относительная необходимость, на третьем – оцениваются угрозы, уязвимости и вероятности риска, на окончательном этапе рассчитываются ожидаемые годовые потери и оценки общих убытков от перерыва в деятельности.

Исходя из изложенного можно заключить, что в настоящее время возникает необходимость в адаптации института тайн к развитию информатизации, в том числе защиты информации в киберпространстве. Наряду с организационно-правовыми мерами обеспечения безопасности информации возрастает роль ее защиты техническими методами, большое значение имеет также учет сведений о средствах, методах, технологиях получения несанкционированного доступа к защищаемым информационным ресурсам, результатов оперативно-розыскной и контрразведывательной деятельности, научных исследований и опытных разработок, иных сведений в области современных информационно-компьютерных технологий и особенностей обстановки в сфере национальной безопасности.

УДК 343.37 + 343.35

***О.В. Маркова***

## ЭЛЕКТРОННЫЕ ДЕНЬГИ И ОТМЫВАНИЕ ПРЕСТУПНЫХ ДОХОДОВ

Обеспечение безопасности финансовой системы государства – одна из важнейших задач ее стабильности и процветания. Стремительное развитие информационно-коммуникационных технологий и социальных сетей, альтернативных платежных систем и инновационных средств платежа, постоянное появление новых продуктов на рынке банковских услуг, дистанционное финансовое обслуживание, несвоевременность и несовершенство правового регулирования этих процессов приводят к тому, что финансовая система становится областью совершения преступных посягательств, противодействовать которым все более затруднительно.

В настоящее время экономические отношения перешли в глобальную электронную среду. Масштабы проведения незаконных финансовых операций, связанных с отмыванием преступных доходов, использованием современных платежных систем, постоянно увеличиваются. Появляется возможность осуществления расчетов между различными субъектами хозяйствования территориально удаленными друг от друга в считанные минуты, что экономит время и позволяет в короткий срок осуществить многочисленные финансовые операции, проверить реальность которых часто невозможно. Речь идет о возникновении и распространении сетевой экономики (networked economy). Современные средства платежа становятся все более мобильными, преступники могут осуществлять доступ к банковским счетам удаленно, быстро реагировать на изменения финансового рынка, контролировать банковские переводы собственных средств. Использование новых телекоммуникационных

систем позволяет создавать целые финансовые альянсы, электронные магазины для реализации преступных финансовых схем. Злоумышленники для заключения криминальных сделок используют возможности социальных сетей, защищенных закрытых чат-каналов, другие возможности интернета и предпочитают оставаться в телекоммуникационных системах для осуществления расчетов. Интернет рассматривается не только как канал получения преступных средств, но и их преобразования, придания правомерного вида.

Несмотря на появление новых платежных продуктов популярными остаются электронные деньги. Законодатель Республики Беларусь определил в ст. 274 Банковского кодекса термин «электронные деньги» – хранящиеся в электронном виде единицы стоимости, выпущенные в обращение в обмен на наличные или безналичные денежные средства и принимаемые в качестве средства платежа при осуществлении расчетов как с лицом, выпустившим в обращение данные единицы стоимости, так и с иными юридическими и физическими лицами, а также выражающие сумму обязательства этого лица по возврату денежных средств любому юридическому или физическому лицу при предъявлении данных единиц стоимости. Электронные деньги находятся в виртуальной области и не обладают каким-либо реальным воплощением, они представляют собой условные единицы. Как у наличных денежных знаков есть серийный номер, который неповторим и уникален, так и у электронных денег есть цифровой номер, который создается специальной математической программой и записывается на жесткий диск электронного устройства, находящегося в распоряжении его владельца, обеспечивая невозможность расплатиться электронными деньгами дважды.

Оборот электронных денег осуществляется только через электронные платежные системы, которые позволяют производить платежи как путем проведения электронных наличных расчетов (WebMoney, Yandex.money и пр.), так и безналичных через виртуальные счета (Assist, Kreditpilot и др.). У ученых до сих пор нет однозначного ответа на вопрос о том, являются ли электронные деньги одной из форм безналичных платежей или новым самостоятельным подвидом, либо это вообще может рассматриваться как тип денежных услуг.

Десятки действующих электронных платежных систем предлагают своим клиентам весь спектр финансовых услуг (открытие счета, хранение и перевод денежных средств, обмен наличных и безналичных денег на электронные и наоборот и др.). В качестве преимуществ использования электронных денег можно назвать следующие: быстрота и всеобщая доступность открытия электронного счета, удаленный доступ к управлению электронным кошельком, простота, мобильность и скорость осуществления расчетов, анонимность держателей электронных средств, низкая стоимость транзакций. Данные преимущества осложняют контроль финансовых операций с использованием электронных денег и выявление фактов отмывания преступных доходов. Перемещение финансовых потоков в короткие сроки усложняет процесс их отслеживания, так как практически не остается следов ни на бумажных носителях, ни в сервере системы. Особенно затруднительно задокументировать преступные схемы по легализации «грязных» денег в ситуациях многосторонних расчетов либо с участниками международных операций, а также при осуществлении многократной анонимной регистрации при осуществлении «мнимых» сделок. Электронные платежные системы располагаются вне национальной юрисдикции, часто переводы связаны с офшорными центрами, что затрудняет сотрудничество с данными государствами и приводит к невозможности принимать эффективные меры по финансовому мониторингу, замораживанию активов и их возвращению. Отсутствие личного контакта между пользователем электронным кошельком и платежной системой не позволяет знать и идентифицировать клиента.

Республика Беларусь как многие государства разрабатывает на законодательном и институциональном уровнях свою систему противодействия легализации средств, полученных преступным путем, в том числе с использованием электронных денег. В настоящее время накоплен огромный мировой опыт правового регулирования сферы обращения и использования электронных средств платежа. Однако использование данного финансового инструмента остается слишком рискованным с позиции возможности использования его для отмывания преступных доходов, особенно в связи с неуклонным возрастанием количества и объема сделок, проходящих через электронные системы. Полноценно законодательно урегулированный рынок электронных денег обеспечит безопасность оказываемых платежных услуг и не снизит их эффективность использования. Современные преобразования телекоммуникационных систем, развитие информационной и электронной инфраструктуры, а также усиление финансового контроля традиционных финансовых инструментов предоставляют преступникам новые неограниченные возможности для отмывания криминальных доходов. Увеличение спроса на цифровые услуги и продукты будет расти дальше. Если ранее в качестве средств платежа в целях легализации преступных материальных ценностей использовались исключительно наличные денежные средства, после безналичные, то в настоящее время активно используются электронные деньги, а также криптовалюта и деривативы. Сегодня задачей любого государства в целях обеспечения экономической безопасности является снижение или минимизация рисков и угроз использования электронных денег для отмывания преступных доходов и повышение прозрачности сделок с данным платежным средством.

УДК 343.985.8

***А.О. Мартынов***

## ИСПОЛЬЗОВАНИЕ СПЕЦИАЛЬНЫХ ЗНАНИЙ В ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ

Одной из негативных форм проявления научно-технического прогресса является развитие противоречащих интересам общества и государства криминальных процессов, опирающихся на последние научно-технические достижения. Преступники становятся более изобретательными, используя все новые способы совершения преступлений, тщательно маскируя следы противоправной деятельности. Методики противодействия указанным выше негативным тенденциям разрабатываются на основе практической деятельности лишь спустя определенное время.