пах прохождения, начиная от профильного министерства (ведомства) и заканчивая конкретной программой или объектом финансирования, включая конечного потребителя. Основной целью мониторинга является выявление любых отклонений от принятых стандартов законности, эффективности, результативности и экономичности управления бюджетными ресурсами с тем, чтобы иметь возможность своевременно исправить ситуацию либо пресечь противоправные деяния, обязать виновных лиц компенсировать нанесенный ущерб, а также предпринять меры для предотвращения аналогичных нарушений в будущем. Сочетание аналитической деятельности с практической работой позволяет выявлять предпосылки и причины не только отдельных правонарушений, но и целых теневых схем, и дает возможность вносить конкретные предложения по совершенствованию законодательства для повышения эффективности в обеспечении экономической безопасности государства.

Одним из направлений совершенствования деятельности по предупреждению экономических преступлений является расширение источников информационного обеспечения. Помимо служебных источников информации в аналитике целесообразно использовать и открытые, при ведении аналитического поиска в интернете получаемые данные дополняются характеризующими сведениями из внутренних источников информации.

Анализ деятельности правоохранительных органов позволяет предположить, что усилятся существующие тенденции криминального внимания к вопросам применения подконтрольных иностранных субъектов хозяйствования для минимизации налоговых платежей. Существует возможность наличия острой проблемы оттока капитала за рубеж, все чаще встречаются случаи противоправного взаимодействия субъектов реального сектора экономики с подозрительными зарубежными фирмами. Так, например, с учетом того, что с 2018 г. латвийские компании платят налог на прибыль только при ее распределении (т. е. нераспределенная прибыль не облагается налогом), в совокупности с отменой запрета на открытие гражданами Республики Беларусь счетов в иностранных банках, возникают предпосылки для внедрения в белорусские бизнес-модели латвийских субъектов хозяйствования, что может повлечь за собой отток капитала в Латвию. В связи с функционированием Единого экономического пространства можно прогнозировать рост числа теневых финансовых операций с целью уклонения от уплаты налогов с использованием реквизитов лжепредпринимательских структур, зарегистрированных на территории государств – участников ЕврАзЭС.

Стандартная процедура получения информации в отношении такой компании путем направления международного запроса может не привести к желаемому результату по ряду объективных и субъективных причин, например, в случае отсутствия соглашения об обмене информацией со страной регистрации субъекта хозяйствования. При наличии соглашения ответ на запрос с учетом всех юридических формальностей может составлять значительный период времени.

В свою очередь, посетив адрес в сети Интернет https://en.wikipedia.org/wiki/ List_of_company_registers, можно установить данные о регистрирующих органах всех государств мира, получив информацию об источниках требуемых сведений. По адресу https://www.lursoft.lv/?l=ru находится коммерческая база данных со сведениями о предприятиях ряда стран, в том числе латвийских (при входе на указанную страницу по умолчанию поиск осуществляется по латвийским субъектам). При этом отдельные характеризующие данные о фирме можно получить бесплатно. Для получения более достоверных сведений о фирмах (имеются сведения только о назначении директоров и управляющих, сведения об учредителях отсутствуют) следует использовать сайт издания «Латвийский Вестник» (https://www.vestnesis.lv/), в котором осуществляется официальное опубликование различных значимых сведений, в том числе касающихся деятельности юридических лиц.

Таким образом, информационно-аналитическое обеспечение является важнейшим элементом организации деятельности правоохранительных органов по предупреждению экономических преступлений, базой для планирования, прогнозирования и принятия оптимальных стратегических и тактических решений. Ключевым направлением внедрения и функционирования успешной аналитики должна стать разработанная система аналитического обеспечения предупреждения экономических преступлений и широкое использование возможностей аналитического поиска; помимо служебных баз данных при осуществлении информационно-аналитической работы целесообразно использовать открытые источники информации. Этому способствует проводимая многими странами политика «открытых данных», которая позволяет законно осуществлять сбор информации о субъектах хозяйствования (особенно зарубежных) за непродолжительное время.

УДК 340

П.В. Лутович

ЗАЩИТА ГОСУДАРСТВЕННЫХ СЕКРЕТОВ В УСЛОВИЯХ ИНФОРМАЦИОННОЙ ОТКРЫТОСТИ БЕЛАРУСИ

В современном мире в условиях глобализации и зарождения информационного общества государства, заинтересованные в научном, технологическом и производственном развитии, находятся перед сложной дилеммой – как сохранить в тайне от потенциальных противников и конкурентов свои военные, научно-технические, иные секреты и не мешать при этом международному научному обмену и взаимодействию. В этой связи институт государственных секретов присутствует в законодательстве большинства стран, имеет национальные различия и много общего в развитых демократиях, но каждой страной применяется самостоятельно. В Республике Беларусь сформированы условия безопасного использования сведений, составляющих государственные секреты. Организованная защита государственных секретов является комплексной, научно обоснованной, апробированной многолетней практикой системой мер, отражающей государственный подход к обеспечению национальной безопасности в информационной сфере.

Сегодня все спецслужбы мира большую часть разведывательной информации черпают из открытых источников. Аналитики, специализирующиеся в области разведки, утверждают, что из газет, журналов, докладов зарубежных «мозговых трестов», материалов научных конференций и т. д. можно получить все сведения, необходимые для представления достаточно

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