посылала ее на сервер преступников, расположенный в Украине. С депозитных счетов крались деньги, «мулы» переправляли их за рубеж.

Новшество заключалось в более качественном, чем когда-либо ранее, заметании следов. Прежде чем грабить банковский счет, программа проверяла величину средств на нем, после чего снимала часть. Точный размер снимаемых средств каждый раз генерировался индивидуально и не превышал размеров счета. Перевод сумм одинакового размера с многих счетов сразу вызовет подозрение, а тут все суммы были разные. Но главной новинкой была подделка веб-страниц банка. Клиент, запрашивавший данные о состоянии счета через компьютер, видел на экране фальшивую страницу, на которой указывался старый (до совершения кражи) остаток средств на счету. Правда могла выясниться лишь при получении выписки через банкомат или при личном обращении в банк.

Успешное функционирование современного общества всецело зависит от того, насколько эффективно организованы и отлажены информационные процессы, протекающие в нем. В этой связи все большее значение для Республики Беларусь приобретает объединение данных процессов в информационное пространство в рамках государства.

Существующие в настоящее время методологические подходы к оценке состояния объектов экономической безопасности в недостаточной степени учитывают особенности формирования информационной среды. Особенно остро проблема развития методологии оценки масштабов экономической и налоговой преступности проявилась в последнее время, когда были критически проанализированы направления формирования экономической безопасности. Безопасность может быть достигнута только тогда, когда будет обеспечена безопасность национальных информационных структур каждой страны мира, а также глобальной информационной инфраструктуры в целом как технологической основы мирового экономического пространства.

Информационные воздействия на экономические процессы, включая финансовую сферу, становятся все более агрессивными. Так, экономический ущерб возникает при воздействии негативной информации на фондовые рынки с одновременной игрой на понижение капитализации предприятий, что связано с их скупкой по низкой цене. При этом распространяется информация негативного характера в отношении конкурента по созданию негативного образа конкурента.

Можно констатировать опасность в виде стремления ряда стран к доминированию в мировом информационном пространстве.

А.П. Пацкевич

ПРОБЛЕМЫ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ДЕЯТЕЛЬНОСТИ ПОДРАЗДЕЛЕНИЙ ПРЕДВАРИТЕЛЬНОГО РАССЛЕДОВАНИЯ

В процессе противодействия преступности подразделениями предварительного расследования используются наиболее действенные научно-методические комплексы раскрытия и расследования разных видов преступлений в различных следственных ситуациях с использованием новейших информационных технологий.

Особую роль при работе с доказательственной базой по уголовным делам выполняют автоматизированные рабочие места (АРМ) следователей, которые отличаются большими функциональными возможностями, включают (либо позволяют легко использовать) в качестве составных частей такие прикладные программы, как текстовые редакторы, электронные таблицы, средства деловой графики и т. п.

Автоматизированное рабочее место представляет собой профессионально ориентированную малую компьютерную систему, предназначенную для автоматизации работ конкретного специалиста. Рассматривать АРМ можно в двух направлениях: технологическом – как автономный, интегрированный с внешними источниками при помощи модема аппаратно-программный комплекс с набором функциональных программ, посредством которых следователь ведет предварительное расследование; в логико-аналитическом – как универсальный пакет программных продуктов, предназначенных для оптимального расследования уголовных дел.

Система АРМ позволяет децентрализовать обработку информации, т. е. решить возможности обработки данных на профессиональном языке следователей.

Назначение АРМ определяется специальным программным обеспечением. При его разработке должны учитываться потребности конкретного пользователя при решении определенных задач. Кроме того, большое внимание следует уделять программному интерфейсу, заданию оптимальных параметров режима диалога пользователя и ЭВМ: они должны быть простыми и доступными в практической деятельности. Вкупе с приемлемым интерфейсом диалогового окна это упростит общение следователя с ЭВМ.

Система АРМ должна быть открытой, гибкой и приспособленной к постоянному развитию и совершенствованию. В состав любого АРМ обязательно входят такие стандартные программные средства, как операционная система, какая-либо системная оболочка или среда, программы-архиваторы, средства диагностики и защитное обеспечение, определяемое специализацией АРМ.

На этапе исследования предметной области АРМ определяются: перечень задач по обработке информации, который должен выполнять на нем специалист; информационная взаимосвязь файлов, которые входят в ее состав; вид экранных форм ввода информации и выходные документы, которые должно формировать АРМ; формы запроса на поиск информации в базе данных АРМ.

Задача совершенствования информационного обеспечения следственно-оперативных групп при проведении следственных действий может успешно решаться посредством создания мобильного автоматизированного рабочего места. Последнее включает в себя ноутбук с необходимым программным обеспечением и периферийным оборудованием, а также средства связи и передачи данных.

Необходимость и целесообразность использования АРМ в расследовании каждого уголовного дела представляется на текущий момент достаточно сомнительной. Полностью доверить машине мыслительную человеческую деятельность недопустимо, так как творческие и логические моменты при этом будут утеряны.

Прототипы сегодняшних АРМ следователей выявляют недостаточную проработанность их как с точки зрения эвристической ценности, так и с позиций сугубо технических. Нередко разработкой подобных программ заняты коллективы, слабо представляющие себе процесс расследования, к сожалению, не имеющие даже малейшего представления о процедуре расследования уголовных дел. Типичными компонентами таких систем являются банки данных по массиву нормативно-правовой информации, касающейся вопросов расследования преступлений и образцов процессуальных документов без возможности их изменения в связи с изменением процессуального законодательства и т. д., и примерами из расследования конкретных уголовных дел для проведения пользователем АРМ неких взаимосвязей и аналогий, которые якобы должны обеспечить формирование следователем оптимальных алгоритмов действий. Либо же система разрабатывается коллективами следователей, имеющими индивидуальные, выработанные практикой наборы определенных задач и решений, которые представляют собой конкретное уголовное дело, что часто неприемлемо для расследования уголовных дел, например, в других регионах с учетом специфики криминогенной обстановки и других внутриведомственных факторов и т. д.

Также не предусмотрен в современных АРМ следователя учет нестандартного или внезапного развития следственной ситуации, в отличие от той, которая была занесена в базу данных АРМ на первоначальном этапе расследования.

Недостатком является отсутствие при применении АРМ так называемой творческой составляющей в процессе расследования, в частности при определении последовательности (вариационности) следственных действий и оперативных мероприятий следователем, которая при использовании ЭВМ утрачивает свою эффективность и не применяется.

На нынешнем этапе электронная компонента самого процесса расследования может быть связана с системами искусственного интеллекта, широко применяемыми в зарубежных странах, которые вообще в будущем в той или иной степени будут вытеснять «человеческий фактор» в расследовании. Ведь не существует абсолютно одинаковых преступлений и потому нельзя научить машину эффективно расследовать каждое строго индивидуализированное происшествие, преступную деятельность.

Перспективным направлением в области развития информационных технологий в расследовании является применение аппаратно-программных средств с использованием современных методов корреляционного, факторного и регрессного анализа, методов аналитического и имитационного моделирования, методов, включающих представление сложных систем и связей, состоящих из отдельных элементов с индивидуальными свойствами, связями и состояниями, что позволяет извлекать собственно оперативно-розыскную информацию и прогнозировать развитие различных ситуаций в преступных группах и сообществах. Использование программных продуктов для прогнозирования развития ситуаций в преступных группах, которые складываются в результате тех или иных действий правоохранительных органов, открывает возможность планировать и оказывать на них целенаправленные информационно-психологические воздействия, как в ходе оперативных мероприятий, так и в ходе следственных действий.

Объектами при использовании логико-математического моделирования могут быть признаки спорных ситуаций, факты, образующие состав преступления и связанные с ними обстоятельства, отношения между предметами и явлениями, признаки следов. Так, моделирование дорожно-транспортных происшествий позволяет решать многие задачи: восстановить границы места происшествия, определить линию столкновения и положения транспорта относительно препятствия в момент контакта, воспроизвести основные фазы и элементы механизма дорожного происшествия.

В первую очередь важна не работа по готовому алгоритму, заданному разработчиком программного средства, а динамическое развитие логики самой задачи, требующей своего разрешения в процессе расследования определенной категории уголовных дел, реализуемых в процессе диалога следователя – пользователя ЭВМ. Подобных резуль-

татов можно достичь лишь при создании и использовании в компьютеризированных системах искусственного интеллекта (экспертных систем), представляющего собой автоматизированные информационные системы, которые на основе своих внутренних ресурсов могут приспосабливаться к возникающей внешней ситуации, определять взаимосвязь между различными факторами, характеризующими эту ситуацию, их место и роль в окружающей систему информационной среде и на основе обработки введенной на первоначальном этапе и вводимой пользователем по запросам системы в процессе ее работы информации и данных вырабатывать набор возможных решений поставленной задачи (задач), снабженных интеллектуальным интерфейсом, позволяющим пользователю обращаться к данным на естественном или профессионально-ориентированном языке.

Общее требование ко всем автоматизированным информационным системам применимо и для АРМ, используемых в раскрытии и расследовании преступлений, – это наличие эффективных механизмов своевременной актуализации в базе данных по расследуемому уголовному делу, т. е. оперативность пополнения изменяющейся информации, складывающейся в результате развития конкретной следственной ситуации.

Таким образом, для эффективного расследования уголовных дел необходимо применять АРМ с расширенными возможностями программных продуктов, направленных на повышение уровня информационно-криминалистического обеспечения служебной деятельности и создание оптимальной информационной структуры аппаратно-программного средства АРМ в деятельности по раскрытию и расследованию преступлений, что позволит качественно и эффективно проводить расследование уголовных дел и индивидуализировать нагрузку на каждого следователя.

Д.В. Перевалов

ПРОЦЕДУРНЫЙ ПОДХОД ОТНЕСЕНИЯ ОБЪЕКТОВ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ ИНФРАСТРУКТУРЫ К КРИТИЧЕСКИ ВАЖНЫМ ОБЪЕКТАМ

В настоящее время доминирующей идеей построения государственной системы защиты информации является создание системы критически важных объектов (КВО), в связи с чем все большую актуальность приобретает проблема их защиты в различных областях (в том числе и в информационно-телекоммуникационной инфраструктуре (ИТИ)) от различного вида угроз. При разработке данной проблематики одним из приоритетных направлений исследования является создание методик для отнесения соответствующих объектов к категории критически важных.

Существуют значительное число подходов к определению понятия КВО в системе ИТИ. Наиболее точным представляется определение такого объекта, предложенное В.В. Стрежневым и А.В. Ениным в проекте Межгосударственного стандарта «Безопасность информации на критически важных объектах информационно-телекоммуникационной инфраструктуры. Основные термины и определения». По их мнению, это объект, нарушение (или прекращение) функционирования которого приводит к чрезвычайной ситуации или к значительным негативным последствиям для обороны, безопасности, международных отношений, экономики, другой сферы хозяйства или инфраструктуры страны, либо для жизнедеятельности населения, проживающего на соответствующей территории, на длительный период времени (п. 2.1.7) [1].

В настоящее время для отнесения объектов к категории критически важных используется в основном методический подход, в основе которого лежит такой критерий, как важность объекта. Формирование такого показателя осуществляется в рамках таких групп, как: субъекты природных монополий, которые ведут деятельность на общегосударственном рынке товара; предприятия оборонно-промышленного комплекса, составляющие научно-технический потенциал страны; предприятия, на которых работают более 10 тыс. человек и т. д. При этом для оценки важности объектов в масштабе указанных групп разрабатывается специальная система рамочных критериев, характеризующихся такими показателями, как: значимость объекта для экономики страны; нанесение ущерба престижу государства, возможные угрозы населению и территориям [2].

Однако в данном случае не решается вопрос о том, каким образом тот или иной объект становится КВО. В связи с этим кроме методического подхода представляется необходимым использовать процедурный подход, который устанавливает соответствующие процедуры по отнесению объекта к КВО в той или иной системе.

Использование процедурного подхода позволяет решать следующие задачи:

учесть особенности функционирования объекта в зависимости от его характеристик при его переводе в категорию КВО;

дифференцировать ресурсы на перевод объекта в категорию КВО;

осуществить нормативное закрепление порядка и процедур включения объекта в систему КВО.

Процедурный подход на современном этапе исследования проблемы целесообразно рассматривать как научно обоснованный и преду-