ситуация-пример S_1, S_2, …, S_n,

решение ситуации-примера U_1, U_2, …, U_n.

Требуется разработать метод, который бы на основе субъективной экспертной информации вычислял веса критериев, проводил ранжирование и принимал решение о предпочтительном выборе ситуации для изменения наилучшим образом оперативной обстановки.

Сложность в реализации заключается в том, что:

в БЗ невозможно предусмотреть все возможные ситуации, складывающиеся в предметной области;

текущая ситуация может отличаться от имеющейся в базе знаний, следовательно, решение для нее также должно быть отличным от известного «решение – пример».

Необходимо разработать способ формализации представления ситуаций и решений, который позволит получать решения для текущих ситуаций на основе формальных преобразований «пример – решение».

Учитывая основные свойства задачи (трудность формализации, субъективность исходной информации, неопределенность цели и т. п.) для определения приоритетов критериев, наиболее подходящим для ее решения является подход, основанный на анализе иерархий. Гибкая методология данного подхода учитывает материальные и нематериальные факторы, позволяет работать как с количественными параметрами, так и с качественными характеристиками, с объективными данными и экспертными оценками.

Метод анализа иерархий использует в качестве языка формализации нечеткую логику.

В соответствии с описанной выше методологией необходимо построить модель задачи в виде некоторой иерархической структуры, разработать алгоритмы вычисления весов (для критериев), разработать алгоритм выбора принятия решений (выбор наиболее предпочтительного решения ситуации-примера). Возможность влиять на характеристики, которые определяют степень достижения цели, формализуется как выбор значения управляющего параметра. При этом управляющий параметр может быть числом, вектором, может быть элементом конечного множества или иметь более сложную математическую природу.

Для оценки возможных решений используются различные критерии. Под критериями понимаются, во-первых, показатели, характеризующие степень приближения к цели каждого из вариантов ее достижения, во-вторых, показатели, служащие для объективного сопоставления различных вариантов решения и выбора из них наиболее эффективного. Критерии могут выражаться в каких-либо показателях использования ресурсов или времени. При выборе и использовании критериев существуют следующие сложности. Во-первых, критерии не всегда могут быть выражены определенными количественными показателями, а во-вторых, чаще всего используется не один критерий выбора альтернатив. Как правило, альтернативы оцениваются по целому комплексу критериев. Для оценки управленческих решений необходимо применять систему критериев.

Необходимость использования совокупности количественных и качественных критериев ставит вопрос о приведении их к «общему знаменателю». Тем самым ставится задача агрегирования частных критериев или выбора одного критерия в качестве основного.

Динамика реальных сложных систем такова, что большинство формальных моделей дают только качественную картину. Например, не существует математических моделей, позволяющих достаточно точно спрогнозировать состояние преступности одноразовым решением. Разнообразные формальные методы управления сложными системами во многих случаях не могут дать однозначных ответов. Хотя процесс построения СППР является очень сложным, тем не менее СППР является инструментом повышения эффективности использования информационных ресурсов в деятельности органов внутренних дел в борьбе с преступностью и по профилактике правонарушений.

УДК 351/354

В.Н. Лебедев

РАЗВИТИЕ СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ОРГАНАХ ВНУТРЕННИХ ДЕЛ

В современном мире право физического лица на личную тайну закреплено конституциями всех развитых государств. Суть этого права заключается в том, что только сам человек, владеющий некими сведениями о себе, может решать, подлежат они разглашению или нет.

В случае неправомерного разглашения таких сведений их владелец имеет право на защиту своих нарушенных интересов. В ряде стран, в том числе в России, неправомерное разглашение персональных данных определенного характера является уголовным преступлением. Однако в судах все чаще рассматриваются споры о разглашении персональных данных (ПДн) физических лиц. Данная проблема, в том числе, связана с широким использованием информационных систем для обработки персональных данных (ИСПДн).

В соответствии с нормами федерального законодательства сведения о гражданах после обработки в органах внутренних дел вносятся в банки данных. Министерство внутренних дел Российской Федерации является оператором, организующим и осуществляющим обработку ПДн, а следовательно, обязано принимать установленные законом ме-

ры для их защиты. С этой целью МВД России создана система защиты ПДн, которая представляет собой совокупность следующих элементов: 1) персональные данные и носители таких данных; 2) должностные лица, подразделения и сотрудники, ответственные за организацию и проведение работ по защите ПДн; 3) способы, техника и средства защиты ПДн; 4) мероприятия, проводимые в целях защиты ПДн. Кратко рассмотрим эти элементы.

Персональные данные, которые обрабатывают органы внутренних дел, определены прежде всего ч. 3 ст. 17 Федерального закона РФ «О полиции», а также нормами других законодательных актов. Кроме того, в различных подразделениях и службах органов внутренних дел (медицинские учреждения, кадровые, финансово-экономические, тыловые подразделения) обрабатываются ПДн сотрудников (работников), а также данные членов их семей.

В соответствии с требованиями приказа МВД России руководители (начальники) территориальных органов МВД России, руководители структурных подразделений территориальных органов МВД России, эксплуатирующие ИСПДн, обеспечивают выполнение правовых, организационных и технических мер, направленных на обеспечение безопасности ПДн, и являются ответственными за соблюдение требований по защите ПДн при их автоматизированной обработке в подчиненном органе внутренних дел.

Кроме указанных выше должностных лиц, ответственными за соблюдение требований по защите ПДн являются администраторы информационных систем персональных данных, пользователи, непосредственно обрабатывающие ПДн, инженерно-технический персонал, имеющий доступ к элементам ИСПДн.

Координацию и контроль деятельности по защите ПДн осуществляет Департамент информационных технологий связи и защиты информации МВД России (ДИТСиЗИ МВД России), в территориальных органах МВД России – подразделения информационных технологий, связи и защиты информации или должностные лица, назначенные ответственными за проведение мероприятий по технической защите ПДн, а также ответственными за организацию обработки ПДн в подразделении.

К способам и методам защиты персональных данных в ИСПДн органов внутренних дел относятся:

способы и методы защиты ПДн от несанкционированного доступа к ПДн (методы и способы защиты информации от несанкционированного доступа);

способы и методы защиты речевой информации, а также информации, представленной в виде информативных электрических сигналов, физических полей, от несанкционированного доступа к ПДн (методы и способы защиты информации от утечки по техническим каналам).

В целях защиты ПДн, обрабатываемых в ИСПДн, применяются средства:

от несанкционированного доступа при передаче по каналам связи сетей общего и (или) международного обмена (средства управления и разграничения доступа пользователей к ПДн; обеспечения регистрации и учета действий с информацией; обеспечения целостности данных; антивирусной защиты; межсетевого экранирования; анализа защищенности; обнаружения вторжений; криптографической защиты ПДн);

от утечки по техническим каналам (генераторы активного акустического, виброакустического и электромагнитного маскирующего зашумления, сетевые помехоподавляющие и телефонные фильтры, а также средства экранирования и заземления и др.).

Выбор средств защиты информации осуществляется в соответствии с требованиями Федеральной службы по техническому и экспертному контролю и ФСБ России: применяемые средства защиты информации должны пройти оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации.

Законодатель определяет некоторые меры, направленные на обеспечение безопасности ПДн. Например, к основным из них относятся: определение угроз безопасности ПДн, применение организационных и технических мер по обеспечению безопасности ПДн, оценка эффективности принимаемых мер по обеспечению безопасности ПДн и др. Содержание организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн устанавливаются ФСБ России и ФСТЭК России в соответствии с их полномочиями.

Мероприятия, проводимы в органах внутренних дел в целях обеспечения безопасности ПДн, можно разделить на две группы:

1. Управленческие (или организационно-управленческие). Направлены на создание системы технической защиты ПДн и управления ею. Ответственными за организацию проведения данных мероприятий являются руководитель территориального органа МВД России и руководители структурных подразделений, обрабатывающих ПДн.

2. Организационно-технические (по обеспечению безопасности ПДн и аттестации ИСПДн по требованиям защиты информации). Обработка ПДн в ИСПДн органов внутренних дел должна осуществляться после завершения работ по созданию системы технической защиты ПДн, аттестации и вводу в эксплуатацию ИСПДн.

Таким образом, мы рассмотрели систему защиты ПДн, существующую в органах внутренних дел Российской Федерации. Однако, как любая организационная система, система защиты ПДн органов внутренних дел требует своего развития и совершенствования. Попробуем предложить основные направления развития данной системы.

1. Совершенствование системы подготовки руководителей в области обработки и защиты ПДн. Как показывает практика, руководители территориальных органов и структурных подразделений далеко не в полной мере обладают необходимыми знаниями и организационными навыками и умениями в области защиты ПДн.

Академия управления МВД России имеет многолетний опыт, есть необходимая материально-техническая база для подготовки руководителей органов внутренних дел разного уровня в области информационной безопасности, в том числе и защиты ПДн.

2. Дальнейшее развитие органов аттестации объектов информатизации на соответствие требованиям безопасности информации, получение территориальными органами МВД России на региональном уровне лицензий на деятельность по технической защите конфиденциальной информации.

3. Максимальная унификация (типизация) информационных систем обработки персональных данных в органах внутренних дел с целью упрощения аттестации на соответствии требованиям защиты информации.

4. Применение в масштабах ведомства унифицированных технических средств и систем защиты ПДн, обрабатываемых в ИСПДн, в целях сокращения расходов на построение систем защиты ИСПДн.

5. Сокращение перечня документов, необходимых для аттестации ИСПДн на соответствие требованиям защиты информации, упрощение самой процедуры аттестации.

В заключение хочется отметить, что эффективная деятельность органов внутренних дел предполагает обеспечение прав и свобод человека и гражданина, что неразрывно связано с обеспечением конфиденциальности личных данных граждан и сведений об их частной жизни, а для этого необходимо совершенствование системы защиты персональных данных в ОВД РФ.

УДК 343

А.Н. Лепёхин

МЕТОДОЛОГИЧЕСКИЕ АСПЕКТЫ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОЙ РАБОТЫ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ

Анализ характера совершаемых преступлений свидетельствует, что современный этап развития общественных отношений характеризуется, несмотря на предпринимаемые правоохранительными органами меры, эволюцией противоправной активности в части появления новых способов криминальной деятельности, коммуникаций между преступ-

никами и смещения акцентов в пользу высокотехнологичных решений достижения преступного результата. Указанные факторы являются серьезным препятствием динамичному социально-экономическому развитию государства.

В этой связи становится актуальным вопрос о формировавании единых и совершенствании имеющихся правовых основ, актуализации, с учетом современных требований, содержания и методики проведения информационно-аналитической работы (ИАР), а также разработки новых подходов ее проведения в правоохранительных органах. При реализации указанных направлений необходимо смещение векторов проведения правоохранительными органами ИАР с информацинной составляющей в пользу совершенствования аналитического обеспечения данной деятельности. Современный этап развития общества характеризуется резким ростом генерируемой информации по различным направлениям, в том числе и имеющей значение для оперативно-служебной деятельности правоохранительных органов. Сегодня в условиях так называемой информационной избыточности вопрос о получении информации (при обеспечении ее свойств – оперативности, достоверности и достаточности) остро не стоит. Более актуальным является ее своевременная аналитическая обработка и принятие на ее основе соотвествующих управленческих решений.

Разработка рекомендаций по правовому регулированию информационно-аналитической работы направлены на формирование и закрепление единых подходов к системе и содержанию нормативных правовых актов, регулирующих отношения в сфере информационно-аналитического обеспечения правоохранительной деятельности, а также на создание необходимых условий для действенной охраны и защиты прав, свобод и законных интересов личности, интересов общества и государства.

Перечисленные обстоятельства позволяют сформировать следующие концептуальные положения рассматриваемой предметной области.

Объектом правового регулирования являются урегулированные законодательством общественные отношения, складывающиеся в сфере правового обеспечения информационно-аналитической деятельности правоохранительных органов в государстве.

Целью подготовки рекомендаций является разработка единых организационно-правовых подходов к информационной и аналитической составляющей правоохранительной деятельности.

Задачами совершенствования и гармонизации законодательства государства, регулирующего отношения в сфере информационно-аналитического обеспечения правоохранительной деятельности, являются: