При этом центральный процессор может обращаться к такому скрипту несколько тысяч раз. Следовательно, если система квотирования настроена неправильно, то такой скрипт за малое время отнимет все системные ресурсы у сервера. Конечно, выход из этой ситуации очевиден – установить определенный лимит на доступ к памяти, но и в этом случае процесс скрипта, достигнув этого лимита, будет находиться в ожидании до тех пор, пока не выгрузит из памяти все старые данные. Поэтому пользователи АСУ будут испытывать существенный недостаток в системных ресурсах.

4. Недостаточная проверка данных пользователя. Этот вид атак также приводит к бесконечному либо длительному циклу или повышенному длительному потреблению процессорных ресурсов АСУ (вплоть до исчерпания процессорных ресурсов) либо выделению большого объема оперативной памяти (вплоть до исчерпания доступной памяти).

5. Провокация. Это атака, которая стремится вызвать ложное срабатывание системы защиты и таким образом привести к недоступности ресурса.

III. Ошибки программирования. Данный тип атак основан на использовании специальных программ (эксплойтов), которые помогают атаковать сложные вычислительные ресурсы АСУ чаще всего из-за ошибок в программном коде, приводящих к обращению к неиспользуемому фрагменту адресного пространства, выполнению недопустимой инструкции или другой необрабатываемой исключительной ситуации, когда происходит аварийное завершение программы-сервера – серверной программы.

1. Недостатки в программном коде. Суть атаки данного вида заключается в том, что злоумышленники ищут ошибки в программном коде какой-либо программы либо операционной системы АСУ, заставляя ее обрабатывать такие исключительные ситуации, которые она обрабатывать не умеет, в результате чего возникают ошибки. Простым примером такой атаки может служить частая передача пакетов, в которой не учитываются спецификации и стандарты RFC-документов. Злоумышленники наблюдают, справляется ли сетевой стек с обработкой исключительных ситуаций. Если не справляется, то передача таких пакетов приводит к панике ядра (kernel panic) или даже к краху всей системы в целом.

К этому виду относится ошибка Ping of death, распространенная еще в 1990-е гг. Длина пакета IPv4 по стандарту RFC 791 IPv4 не может превышать 65 535 байт. При этом на атакуемый сервер АСУ посылается ICMP-пакет большей длины, предварительно разбитый на части, в результате чего на сервере от такого пакета переполняется буфер.

2. Переполнение буфера. Переполнение буфера возникает и в том случае, если программа из-за ошибки программиста записывает данные за пределами буфера. Например, программист написал приложение для обмена данными по сети, которое работает по какому-либо протоколу. В этом протоколе строго указано, что определенное поле пакета максимум может содержать 65 536 байт данных. Однако после тестирования приложения оказалось, что в ее клиентской части сети в это поле нет необходимости помещать данные, размер которых больше 255 байт. Поэтому и серверная часть примет не более 255 байт. Далее злоумышленник изменяет код приложения так, что клиентская часть отправляет все допустимые по протоколу 65 536 байт, но сервер к их приему не готов. Из-за этого возникает переполнение буфера, и пользователи АСУ не могут получить доступ к приложению.

3. DoS-атака на уязвимости в программном обеспечении на DNS-серверах. В процессе этой атаки злоумышленник осуществляет подмену IP-адреса DNS-сервера домена АСУ. После чего атакуемый при запросе HTML-страницы попадает либо в «черную дыру» (если IP-адрес был заменен на несуществующий), либо прямиком на сервер злоумышленника. Второй случай чреват более серьезными последствиями, поскольку злоумышленник легко может получить доступ к информационным ресурсам АСУ.

Из вышеизложенного можно определить существование различных видов DoS-атак. К основным их разновидностям относятся насыщение полосы пропускания, недостаток ресурсов, ошибки программирования. Каждый тип угроз характеризуется специфическим способом осуществления и причинами возникновения DoS-условий.

УДК 004 + 351.74/76 + 623.71

А.В. Железняков

ПРИМЕНЕНИЕ СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ПРИ РАЗРАБОТКЕ ПЛАНА КОМПЛЕКСНОГО ИСПОЛЬЗОВАНИЯ СИЛ И СРЕДСТВ

В процессе управления подразделениями внутренних войск МВД Республики Беларусь возникает необходимость в выполнении ряда расчетных задач, обеспечивающих подготовку и планирование действий приданных сил. Принимаемые решения определяются опытом ответственного лица и реальным знанием местности района ответственности. В то же время при организации управления подчиненными си-

лами, особенно при осложнении обстановки, необходимо владеть информацией о географических объектах (здания, сооружения, транспортные магистрали и инженерные коммуникации, общественные места, лесные массивы и т. д.). Необходимость обрабатывать большой объем информации о местности, труднообозримой и плохо представляемой по карте, приводит к недопустимым временным затратам. В результате принимаемые решения могут быть недостаточно обоснованными, а следовательно, не обеспечивать эффективное выполнение поставленной задачи.

Исследования показывают, что внедрение средств автоматизации и современных информационных технологий в процесс управления дает реальную возможность повысить эффективность принимаемых решений, оперативность и качество управления. Интеграция геоинформационных систем в автоматизированные системы управления войсками обеспечит поддержку принятия более эффективных решений и их реализацию.

Одной из задач обработки цифровой картографической информации (цифровая карта или цифровой план местности) в целях повышения эффективности действий войсковых нарядов по охране общественного порядка (ООП) и обеспечению общественной безопасности (ООБ) является построение маршрутов патрулирования. Это предусмотрено разработкой плана комплексного использования сил и средств ООП, в котором определяются все маршруты войсковых нарядов, закрепленных за территориальным органом внутренних дел (ОВД).

Так, при патрулировании в населенном пункте имеет место выбор маршрута с максимальной площадью просматриваемой территории и минимальным временем нахождения на маршруте при средней скорости движения патруля (войскового наряда). При этом могут быть определены пункты, обязательные для посещения (места скопления граждан, места нахождения источников повышенной опасности, площади, вокзалы, аэропорты, рынки, станции метрополитена, объекты военного назначения, а также прилегающие к ним территории и т. д.). Следует учесть, что в одном районе службу несут несколько патрулей, следовательно, есть следующие ограничения: траектории маршрутов патрулирования не должны совпадать, однако пересечение допускается; интегрированные зоны видимости должны иметь как можно меньшую площадь перекрытия либо разнесены по времени.

Корректировка маршрутов осуществляется: в случае изменения криминогенной обстановки на территории, перераспределения сил и средств, при введении различных планов специальных мероприятий, строительства новых жилых массивов, торговых и развлекательных заведений и т. д.

Под маршрутом понимается передвижение войскового наряда от начальной точки $S_0(x,y)$ к конечной $S_K(x,y)$. А при построении маршрута возврата из точки $S_K(x,y)$ в точку $S_0(x,y)$ необходимо максимизировать площадь просматриваемой территории с минимизацией времени нахождения на маршруте и при этом избежать наложения или пересечения интегрированных зон видимости либо свести их к минимуму. Если принять среднюю скорость V_{cp} движения войскового наряда на всех участках одинаковой, то минимизация времени нахождения сводится к построению кратчайшего маршрута от начальной точки $S_0(x,y)$ к конечной $S_K(x,y)$.

Используя теорию графов, задачу поиска кратчайшего маршрута можно сформулировать следующим образом: на местности задан граф $G=(V,E)$ с двумя выделенными вершинами $p_0, q_0 \in V$, длины $l(e) \in N^+$ и веса $a(e) \in N^+$ для всех ребер $e \in E$. Необходимо найти в G простой путь из p_0 в q_0 с минимальным значением длины L и веса A. При этом под простым следует понимать такой путь, в котором ни одна вершина графа не встречается дважды.

В аналитическом виде задача записывается следующим образом:

$$\Theta = \sum_{i=1}^{k} A(v_i) + \sum_{i=1}^{k-1} L(v_i, v_{i+1}), \qquad (1)$$

где Θ – показатель эффективности найденного маршрута, который требуется оптимизировать; $\{v_i\}$ – вершины графа, через которые проходит маршрут, $i=\overline{1,k}$; k – число вершин, через которые проходит маршрут; $A(v_i)$ – функционал, в соответствии с которым вычисляется вес в вершине графа v_i; $L(v_i, v_{i+1})$ – функционал, определяющий длину ребра из вершины v_i в вершину v_{i+1}.

Вес вершин графа вычисляется в соответствии с функционалом $A(\bullet)$ в результате оценки местности и определяет соответствие дискрет местности предъявленной системе требований к маршруту.

В общем случае вес вершины будет определяться шагом дискретизации Δd и наличием тех или иных географических объектов и элементов обстановки в соответствующей дискрете местности, а также в некоторой окрестности рассматриваемой дискреты.

Для вычисления веса вершины графа необходимо сопоставить объекты, присутствующие в дискрете, с критичными для решаемой задачи объектами, которые определяются системой требований (критериев), предъявляемых к маршруту:

$$A(v_i) = A(\Delta d, P_i, \Omega'), \qquad (2)$$

где Δd – размер шага дискретизации; P_i – множество объектов местности и обстановки, присутствующих в дискрете, соответствующей вершине графа v_i, $i=\overline{1,k}$; Ω' – множество критичных для решаемой задачи объектов местности и обстановки.

С учетом применения матричной модели местности длина маршрута между вершинами графа v_i и v_{i+1} вычисляется в соответствии с выражением:

$$L(v_i, v_{i+1}) = \sqrt{(\Delta d \cdot \eta)^2 + h^2(v_i, v_{i+1})}, \qquad (3)$$

где

$$\eta = \begin{cases} \sqrt{2}, \text{если перемещение между дискретами осуществляется по диагонали,} \\ 1, \text{ во всех остальных случаях.} \end{cases}$$

– коэффициент, учитывающий направление перемещения между дискретами; $h(v_i, v_{i+1})$ – перепад высот в дискретах местности, соответствующих вершинам графа v_i и v_{i+1}.

Оптимизация первого слагаемого выражения (1) достигается благодаря прохождению маршрута по местности, соответствующей требованиям, предъявленным к маршруту. Оптимизация второго слагаемого достигается путем выбора из равных по значению первого слагаемого маршрутов самого короткого по протяженности. Отметим, что в данной постановке задачи не ставится акцент на минимизацию или максимизацию слагаемых, а все ограничивается лишь понятием «оптимизация», что позволяет более гибко использовать разрабатываемую модель как для нахождения наилучших маршрутов, так и для оценки наихудших вариантов.

Таким образом, если обозначить через вектор $\overline{V}$ множество вершин графа v_i, через которые проходит маршрут, то задача поиска оптимального маршрута сводится к поиску вектора $\overline{V}^*$, при котором достигается оптимальное значение показателя эффективности маршрута:

$$\overline{V}^* = \arg \underset{\overline{V} \in V}{\text{opt}} \{A(\overline{V}) + L(\overline{V})\}, \qquad (4)$$

где V – множество вершин, через которые может проходить маршрут.

Исходя из вышеизложенного, решение задачи поиска оптимального маршрута состоит из двух этапов:

на первом (подготовительном) этапе осуществляется оценка обстановки и выделение участков местности, соответствующих выражению (1), по которым может проходить искомый маршрут;

на втором (оптимизационном) этапе осуществляется нахождение оптимального маршрута в соответствии с выражением (4) и с учетом системы ограничений.

Эта задача решается построением интегрированной зоны видимости на основе суммирования зон видимости на каждом условном шаге перемещения войскового наряда от начальной к конечной точке.

УДК 343

В.Ф. Кетурко

ПРОБЛЕМЫ ИНФОРМАТИЗАЦИИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ РЕСПУБЛИКИ БЕЛАРУСЬ

Современный период развития органов внутренних дел характеризуется расширением использования современных информационных технологий в целях достижения более высокого качества, изменения содержания и характера труда сотрудников. Благодаря автоматизации целого ряда информационных процессов сотрудники ОВД освобождаются от рутинных, трудоемких операций.

В то же время, несмотря на положительные примеры использования современных информационных технологий в ОВД, практика показывает, что многие теоретические, методологические, организационные, правовые и технические вопросы еще требуют своего разрешения.

Наиболее актуальными являются проблемы правового регулирования процессов информатизации в правоохранительной сфере. Необходимо признать, что информатизация ОВД и насыщение ее современными информационными технологиями в настоящее время не обеспечены законодательной базой в достаточной степени. Несмотря на принятие ряда ведомственных нормативных правовых актов, затрагивающих отдельные аспекты данной проблемы, детально проработанной нормативной правовой базы информатизации, которая отвечала бы современным условиям, до сих пор не создано.

Хотелось бы подчеркнуть, что комплексное исследование правовых аспектов информатизации правоохранительной сферы будет способствовать выработке конструктивных предложений по существенному повышению эффективности управления всеми правоохранительными органами и ОВД в частности.

В Республике Беларусь политика информатизации начала формироваться с начала 90-х гг. XX в. В 1991 г. Совет Министров Республики Беларусь принял Программу информатизации на 1991–1995 гг. и на период до 2000 г. Впервые о проблеме информатизации в правоохра-