Использование байесовых сетей для оценки террористических рисков и выбора оптимальной стратегии противодействия террористической угрозе.

Н.А.Махутов. Д.О.Резников

Аннотация.

В статье представлен подход к оценке террористического риска, основанный на использовании байесовых сетей и теории игр. Предложена трехсторонняя модель, позволяющая учесть способность террористов осуществлять сознательный выбор сценария атаки на основе анализа уязвимости объекта по отношению к выбранному сценарию атаки и оценки величины ущерба, ожидаемого в случае успешной реализации атаки. Кроме того, представленная модель позволяет проводить оценку эффективности различных вариантов мер противодействия террористической угрозе.

1. Особенности оценки террористических рисков и требования к математически моделям, описывающим террористические угрозы.

Отличительные особенности террористических рисков (по сравнению с рисками природных и техногенных катастроф) обуславливаются способностью террористов осуществлять сознательный выбор сценария террористической атаки. Этот выбор основывается на рациональной оценке: (1) уязвимости рассматриваемого объекта по отношению к различным сценариям атаки и (2) величин ущербов, ожидаемых при реализации различных сценариев атаки. Принимаемые террористами решения базируются на принципе минимакса, заключающемся в стремлении нанести обществу максимальный ущерб при минимальном расходовании ресурсов и минимальном риске обнаружения и ликвидации организации (то есть, на стремлении обеспечить максимальную эффективность атаки). При этом террористы способны реагировать на действия антитеррористических сил, извлекать уроки из опыта предыдущих атак и корректировать тем самым свои действия. Дополнительные сложности, с которыми приходится сталкиваться при оценке террористических рисков, связаны с тем обстоятельством, что система ценностей террористов (т.е. их функция полезности) заметно отличается от традиционной, а система их мотивационных установок, часто оказывается не вполне понятной даже специалистам.

Для задач, связанных с оценкой и управлением террористическими рисками, характерны:

- высокий уровень неопределенности, обусловленный недостатком знаний о намерениях террористов, о их интеллектуальном потенциале и организационно-технических ресурсах, о преследуемых ими целях и их системе ценностей;
- фрагментарность и (часто) засекреченность данных, получаемых из различных источников и имеющих различную природу: статистическая информация, экспертные оценки, оперативная информация, полученная от спецслужб;
- динамический характер террористических рисков.

Разрабатываемая математическая модель оценки террористического риска для рассматриваемого объекта должна отвечать следующим требованиям:

- Модель должна обеспечивать проведение оценок и принятие решений при наличии высокого уровня неопределенности.
- Модель должна быть многосторонней: то есть рассматривать ситуацию как с точки зрения террористов, так и с точки зрения антитеррористических сил. При этом она должна позволять описывать динамическое взаимодействие этих сторон, каждая из которых руководствуется своей стратегией и способна реагировать на действия противника. Кроме того, модель должна позволять учитывать способность террористов выбирать сценарий атаки, обеспечивающий ее максимальную эффективность атаки. То есть предусматривать наличие обратных связей между уязвимостью системы по отношению к рассматриваемому сценарию атаки (а также ожидаемого ущерба) и вероятностью того, что этот сценарий атаки будет избран террористами[1].

[1] Использование двухсторонних моделей, описывающих террористическую и антитеррористическую стороны конфликта, подробно рассмотрено в работе [15]

- В части модели, характеризующей анализ ситуации и принятие решений террористами (часть 1 модели), должна проводиться оценка целей и системы ценностей террористов, их ресурсов, интеллектуального и организационно-технического потенциала, идентификация базовых сценариев осуществления террористических атак против рассматриваемого объекта, а также оценка вероятности реализации различных сценариев террористических атак, исходя из функции полезности, которой (по мнению аналитиков антитеррористических сил) должны руководствоваться террористы.
- Блоки модели, описывающие ситуацию с позиций антитеррористической стороны, помимо собственно оценки уязвимости объекта и эффективности систем защиты должны также использовать результаты, полученные на основе анализа террористической части модели, (а именно, вероятности реализации различных сценариев атак со стороны террористов) для определения наиболее эффективных мер противодействия террористической угрозе. При этом следует учитывать возможность взаимодействия различных сил, противостоящих террористической угрозе, и обмена информацией между ними.
- Модель должна быть динамической, то есть позволять описывать изменение параметров системы (объекта), внешней среды, а также спектра и интенсивности террористических угроз.

Перечисленные требования обуславливают целесообразность привлечения аппарата теории игр [9,14, 19, 20] и байесовых сетей [3,4,5,6,7, 12], которые позволяют: (а) учесть независимость действий и рациональные стратегии поведения террористической и антитеррористической сторон; (б) оценить ситуацию в условиях высокого уровня неопределенности, (в) обеспечить учет информации, получаемой из различных источников (в том числе периодически поступающей информации о состоянии отдельных переменных модели), тем самым, давая возможность получать уточненные апостериорные оценки вероятностей состояний других переменных модели.

Научно-методические аспекты и прикладные разработки стали предметом совместного анализа в рамках программы противодействия технологическому терроризму, реализуемой совместно Российской академией наук и Национальными академиями наук США [5, 24] и научной программы НАТО «Наука ради мира» [25].

2. Использование теории игр при анализе террористических рисков.

Традиционные вероятностные методы, используемые при моделировании ЧС, инициируемых природно-техногенными катастрофами [1], в чистом виде не позволяют описать террористические сценарии инициирования ЧС, поскольку не учитывают намерения террористов, сознательный и рациональный характер их действий, определяющий выбор того сценария атаки, который обеспечивают ее максимальную эффективность [22, 23]. Поэтому в существующие вероятностные модели развития ЧС должен быть включен аппарат теории игр, позволяющий учитывать рациональный характер поведения террористов, и проводить оценки вероятности осуществления различных сценариев террористических атак.

При рассмотрении террористической угрозы наиболее сложным является определение стратегии поведения террористов и, в частности, вероятность выбора ими того, или иного сценария атаки [21].

Поскольку террористы способны осуществлять сознательный выбор между различными сценариями атаки, то наиболее вероятным оказывается сценарий, который обеспечивает нанесение обществу максимального ущерба при минимальных затратах на осуществление атаки и максимальной вероятности ее успеха. Таким образом, между террористической угрозой для рассматриваемого объекта, с одной стороны, и его уязвимостью и величиной ущерба, ожидаемого в случае успешной реализации атаки, с другой стороны, существуют сильные обратные связи, обусловленные упомянутой выше способностью террористов выбирать сценарий атаки, принимая во внимание как свои собственные ресурсы, так и действия и возможности антитеррористических сил.

Для описания этой обратной связи в количественный анализ риска должна быть включена математическая теория игр, которая предоставляет аналитику математический аппарат для выбора стратегии в конфликтной ситуации и позволяет использовать подходы математического моделирования в целях выработки лучших вариантов действий в условиях неопределенности и

возможности противодействия со стороны другой стороны конфликта. Целесообразность привлечения теории игр к проведению оценки террористических рисков, обуславливается тем, что она позволяет описать:

(а) Динамическое взаимодействие между террористической организацией и антитеррористическими силами.

(б) Рациональные действия обеих сторон, каждая из которых стремится действовать с учетом того, как, по ее мнению, будет действовать и реагировать противник.

(в) Стремление максимизировать результат при имеющихся ограничениях.

(г) Принятие решений в ситуации неопределенности, связанной с деятельностью противной стороны.

В основе теории игр лежит принцип минимакса, который состоит в том, что каждая из противостоящих сторон действует таким образом, чтобы минимизировать свой максимальный ущерб. Этот принцип весьма консервативен, поскольку он исходит из того, что противная сторона будет выбирать наилучший из возможных вариантов действий, избегая необоснованных рисков. Теория игр базируется на том, что при выборе стратегии своего поведения участники игры рациональны и разумны. Эти правила поведения вполне соответствуют правилам, по которым развивается соперничество террористических организаций и антитеррористических сил.

Следует отметить, что для того, чтобы использовать теорию игр при построении модели оценки террористического риска, необходимо понимать рациональность не в обыденном смысле этого слова, а обратиться к математическому определению рационального поведения, под которым понимают действия, которые совершаются в соответствии с определенными правилами предпочтения. При этом совершенно не обязательно, что террористы ориентируются лишь на нанесение материального ущерба. Во многом цели террористов лежат в области психологии: ведение «войны с неверными», провоцирование паники среди мирного населения и др. Также не обязательно, чтобы правила предпочтения террористов соответствовали правилам предпочтения, которые действуют для остального общества.

3. Байесовые сети и диаграммы влияния.

Байесовые сети.

Байесовые сети представляют собой графовые модели причинно-следственных отношений между случайными переменными. Каждый узел графа соответствует случайной переменной, фигурирующей в модели, а связи отражают вероятностные соотношения между переменными. Байесовые сети позволяют объединять эмпирические частоты появлений различных значений (состояний) случайных переменных, субъективные оценки «ожиданий» и теоретические представления о математических вероятностях тех или иных следствий из априорной информации. Это свойство байесовых сетей является их важным практическим преимуществом и отличает байесовые сети от других методик моделирования [3, 4, 6, 17].

Байесовые сети строятся на основе следующих элементов и принципов:

- множество случайных переменных и направленных связей между ними;
- каждая переменная может принимать одно из конечного множества взаимоисключающих значений
- переменные вместе со связями образуют ориентированный граф без циклов;
- каждой переменной потомку x_i с переменными-родителями π_i приписывается таблица условных вероятностей $P(x_i \mid \pi_1, \pi_2, ..., \pi_n)$

Байесовые сети широко используются для представления данных и обоснования в условиях неопределенности. Неопределенности, связанные с взаимным влиянием между переменными определяются локальными таблицами условных вероятностей $P(x_i \mid \pi_1, \pi_2, ..., \pi_n)$, построенными для каждого узла x_i, где $\pi_1, \pi_2, ..., \pi_n$ –совокупность, так называемых, родителей узла x_i. Для байесовых сетей вводится допущение об условной независимости, которое заключается в том, что значения переменной x_i при условии, что ее родители π_i принимают определенные значения, не зависят от всех других переменных, за исключением своих «потомков».

Отсутствие связи между двумя переменными интерпретируется как утверждение об условной независимости (т.е. утверждается, что две переменные являются независимыми, при условии, что определенное подмножество переменных модели принимает фиксированные значения). Для каждой переменной, которая не имеет родителей, должно быть задано априорное распределение вероятности. Для каждой переменной, имеющей родителей, должна быть задана таблица условных вероятностей ее нахождения в различных состояниях, при любых возможных комбинациях состояний родителей.

Сетевая структура наряду с таблицами условных вероятностей, соответствующих каждому из узлов, определяет совместные вероятностные распределения всех переменных модели. Графическая структура байесовой сети позволяет получить однозначное представление взаимосвязей между переменными. Это обстоятельство наряду с допущением об условной независимости обуславливает наличие наиболее важного свойства байесовых сетей:

Совместная функция распределения вероятностей переменных $X = (x_1,..., x_k)$ может быть разбита на множители, представляющие собой условные вероятности, заданные в сети.

$$P(X = x) = \prod_{i=1}^{k} P(x_i \mid \pi_1, \pi_2,..., \pi_n) \qquad (1)$$

Был разработан ряд точных и приближенных алгоритмов, позволяющих вычислять апостериорные вероятности значений переменных модели при условии наличия определенных сведений о значениях других переменных модели.

Диаграммы влияния.

Для решения задач, связанных с принятием решений, используются диаграммы влияния, которые являются расширением байесовых сетей и включают помимо узлов, характеризующих состояние случайных переменных (*случайных узлов*), два дополнительные типа узлов: узлы выбора вариантов решений (*узлы решения*) и узлы оценки полезности вариантов решений (*узлы полезности*). Диаграммы влияния позволяют аналитику решать различные задачи, связанные с принятием решений: в частности, проводить вычисление ожидаемой полезности, при наличии некоторых сведений о состоянии переменных модели и сделанном выборе варианта действий, а также осуществлять поиск оптимального варианта действий [3, 8, 10].

Узел решения связан с теми случайными узлами, вероятностное распределение которых прямо зависит от варианта принятия решения. Значение каждой переменной-решения не определяется вероятностно состоянием его предшественников, а задается извне лицом, принимающим решения, исходя из преследуемых им целей и критериев оптимизации.

Узел полезности характеризует случайную величину ожидаемой полезности, которая будет получена в результате принятого решения. Также как и для других случайных переменных (узлов), для узла полезности задается таблица значений полезности для всех возможных сочетаний узлов-родителей. Каждый узел полезности характеризуется функцией полезности, которая отражает полезность принятого решения в зависимости от состояний узлов-родителей.

Пусть $S = \{s_1, s_2,..., s_n\}$ - совокупность взаимоисключающих вариантов действий (например, возможных сценариев осуществления атаки), $V = \{v_0, v_1, v_2,..., v_m\}$ – совокупность состояний определяющей переменной модели. Применительно к рассматриваемой задаче, определяющей переменной является состояние объекта после атаки, тогда переменная V может принимать следующие значения: $V = v_0$ - объект не поврежден, $V = v_1$ - объекту нанесена 1-ая степень повреждения, $V = v_2$ - объекту нанесена 2-ая степень повреждения и т.д., $V = v_m$ - объекту нанесена m -ая степень повреждения.

Для того чтобы оценить каждый из вариантов из действий s_i, необходима таблица полезности $Ut(s_i, v_j)$, позволяющая оценить величину полезности для всех возможных сочетаний вариантов действий и значений, принимаемых определяющей переменной:

Каждый из сценариев атаки s_i, характеризуется следующими параметрами:

$P(V = v_j \mid S = s_i)$ $j = 1,2,\ldots,m$- условные вероятности нанесения объекту j-ой степени повреждения в случае реализации i-го сценария атаки, $W(s_i; v_j)$- ущерб, в случае успешной реализации i-го сценария атаки и нанесения объекту j-ой степени повреждения, $Z(s_i)$ - затраты на подготовку и проведение i-го сценария атаки.

Матрица полезности принимает вид:

$$Ut(s_i; v_j) = \begin{bmatrix} W(s_1; v_0) - Z(s_1) & W(s_1; v_1) - Z(s_1) & \cdots & W(s_1; v_m) - Z(s_1) \\ W(s_2; v_0) - Z(s_2) & W(s_2; v_1) - Z(s_2) & \cdots & W(s_2; v_m) - Z(s_2) \\ & \cdot \quad \cdot \quad \cdot & & \\ W(s_n; v_0) - Z(s_n) & W(s_n; v_1) - Z(s_n) & \cdots & W(s_n; v_m) - Z(s_n) \end{bmatrix} \quad (2)$$

Значение ожидаемой полезности при выборе i-го сценария атаки, определяется как:

$$EU(s_i) = \sum_{j=0}^{m} \left[Ut(s_i; v_j) \times P(V = v_j \mid S = s_i) \right] \quad (i = 1, 2, \ldots, n) \quad (3)$$

В простейшем случае могут быть выделены два состояния объекта после атаки: «объект не поврежден» ($V = v_0$) и «объект поврежден» ($V = v_1$).Кроме того, будем считать, что в случае если в результате атаки объект оказался не поврежден, то ущерб равен нулю: $W(s_i; v_0) = 0$. Поскольку рассматривается только одна степень повреждения объекта, то ожидаемый ущерб будет зависеть только от избранного сценария атаки $W(s_i) \equiv W(s_i; v_1)$

Тогда матрица полезности принимает вид:

$$Ut(s_i; v_j) = \begin{bmatrix} -Z(s_1) & W(s_1; v_1) - Z(s_1) \\ -Z(s_2) & W(s_2; v_1) - Z(s_2) \\ & \cdot \quad \cdot \quad \cdot \\ -Z(s_n) & W(s_n; v_1) - Z(s_n) \end{bmatrix} \quad (4)$$

Подсчитаем значение ожидаемой полезности для этого случая:

$EU(s_i) = -Z(s_i) \cdot P(V = v_0 \mid S = s_i) + [W(s_i; v_1) - Z(s_i)] \cdot P(V = v_0 \mid S = s_i)$

Поскольку события $V = v_0$ и $V = v_1$ образуют полную группу событий, то

$P(V = v_0 \mid S = s_i) + P(V = v_1 \mid S = s_i) = 1$, тогда

$$EU(s_i) = W(s_i; v_1) \cdot P(V = v_1 \mid S = s_i) - Z(s_i) \quad (5)$$

Условные вероятности $P(V = v_j \mid S = s_i)$ вычисляются с помощью специальных алгоритмов, на основе таблиц условных вероятностей для переменных сети при условии выбора сценария s_i. В примерах, представленных в данной статье, использовался программный комплекс GeNie 2.0, разработанный в Питсбургском университет (США) и реализующий различные точные и приближенные алгоритмы расчета.

Проблема поиска наиболее эффективного сценария атаки решается путем определения сценария, который максимизирует ожидаемую полезность согласно выражению (3) или (5).

4. Трехстороння модель для оценки риска террористической атаки против некоторого объекта.

На рис. 1. представлена трехсторонняя модель, состоящая из трех графов. Граф 1 представляет собой диаграмму влияния, описывающую ситуацию принятия решения о выборе сценария атаки с точки зрения террористической организации. Эта диаграмма составляется аналитиками службы защиты объекта, которые, пытаясь рассуждать с позиций террористов (играя за противника), стремятся оценить значения ожидаемой полезности для террористов при реализации различных сценариев атаки. Полученные значения позволяют далее оценить вероятности осуществления различных сценариев атаки. Указанные вероятности

используются в при построении графов 2 и 3, которые характеризуют соответственно принятие решений о выборе мероприятий по противодействию террористической угрозе на уровне службы защиты рассматриваемого объекта (граф 2) и на уровне муниципальных властей, на территории которых размещается указанный объект(граф 3). Следует иметь в виду, что администрация объекта и муниципальные власти могут обмениваться информацией и координировать свои действия, т.е. являются союзниками в игре.

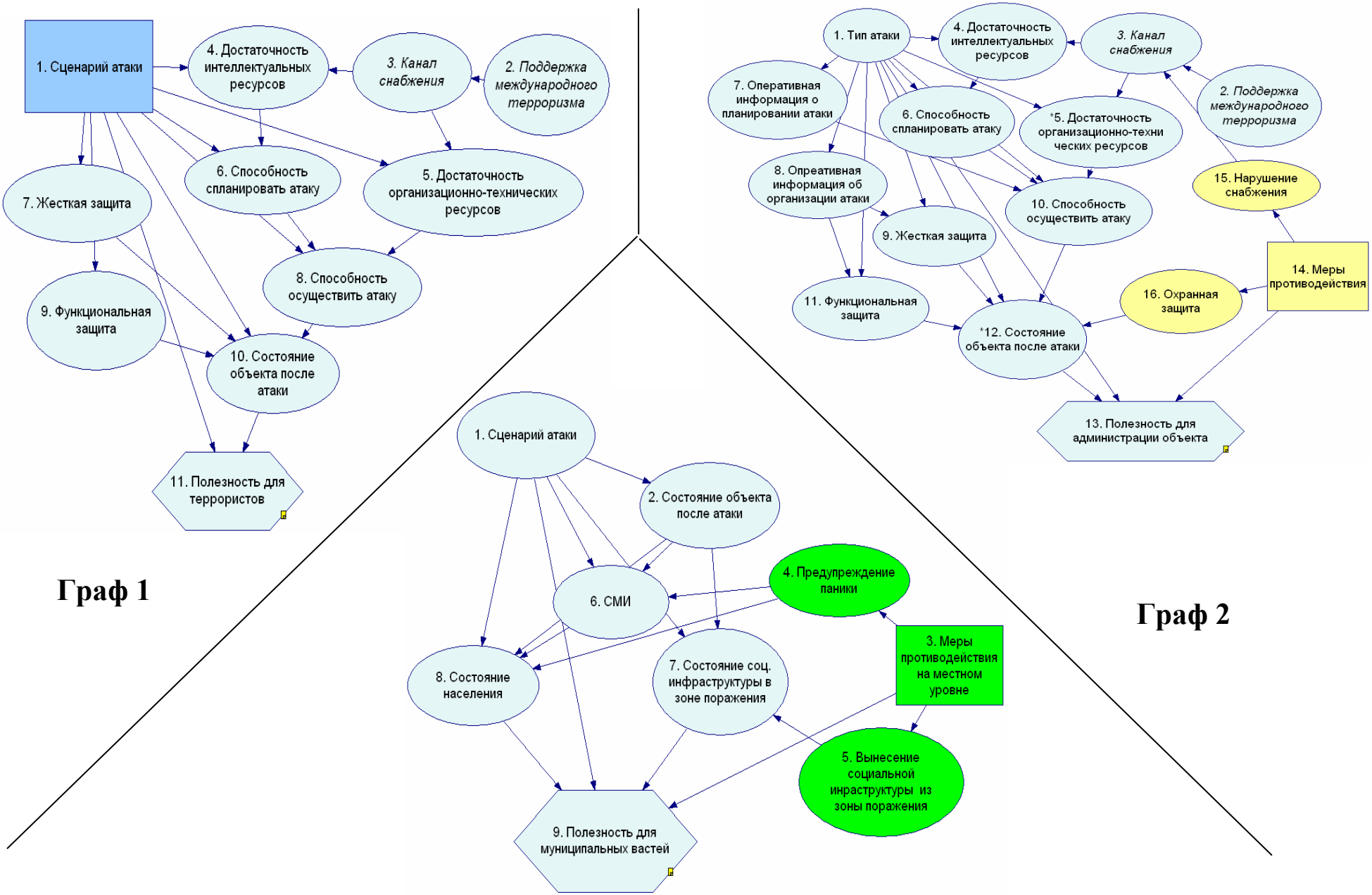

Рис. 1Трехстороння модель оценки террористического риска

Сходства и различия между графами, объясняются тем, что они описывают одну и туже задачу, но с разных позиций. Различия между графами обусловлены, в частности, различным уровнем неопределенности относительно состояния отдельных узлов (состояние одного и того же узла, например, узла, характеризующего ресурсы террористической организации, может быть достоверно известно террористам, и рассматриваться антитеррористическими силами как случайная величина для). Соответственно отличаются и оценки вероятностных связей между переменными задачи (т.е. таблицы условных вероятностей для трех графов). Кроме того, некоторые параметры задачи, могут вообще не учитываться одной из сторон, но в тоже время быть весьма важными для другой. Принципиально отличаются и узлы полезности каждого из графов, поскольку функции полезности террористов, администрации объекта и муниципальных властей могут учитывать совершенно различные факторы: террористы, например, могут ориентироваться прежде всего на нанесение первичного ущерба и на затраты, необходимые для осуществления атаки, в то время как для администрации объекта, функция полезности, должна включать также вторичные ущербы, а также затраты на реализацию различных защитных мер. Функция полезности для муниципальных властей должна, в первую очередь, учитывать ущерб, наносимый населению и инфраструктуре территорий, прилегающих к площадке размещения объекта.

4.1 Построение диаграммы влияния, характеризующей ситуацию с точки зрения террористов.

Рассмотрим сначала граф 1 интегральной модели. Переменные, включенные в граф, представлены в таблице 1.

Таблица 1.

Узлы диаграммы влияния, характеризующие ситуацию с точки зрения террористов.

Наименование переменной	**Тип узла**	**Обозна-чение**	**Принимаемые значения (возможные состояния узлов)**
1. Сценарий террористической атаки.	Узел решения	S	Сценарий 1, Сценарий 2, Сценарий 3
2. Наличие поддержки международных террористических организаций.	Случайный узел	MT	Да/нет
3. Функционирование канала доставки ресурсов для террористической организации.	Случайный узел	KS	Действует/не действует
4. Достаточность у террористов интеллектуальных ресурсов, чтобы спланировать атаку.	Случайный узел	IR	Да/нет
5. Достаточность у террористов организационно-технического потенциала ресурсов, чтобы осуществить атаку.	Случайный узел	TR	Да/нет
6. Способность террористической организации спланировать атаку.	Случайный узел	PA	Да/нет
7. Срабатывание системы жесткой защиты объекта.	Случайный узел	GZ	Да/нет
8. Способность террористической организации осуществить атаку.	Случайный узел	OA	Да/нет
9. Срабатывание системы функциональной защиты.	Случайный узел	FZ	Действует / не действует
10. Состояние объекта после атаки	Случайный узел	*V*	Объект не поврежден Нанесена 1-ая степень повреждения Нанесена 2-ая степень повреждения ….. Нанесена *m*-ая степень повреждения
11. Ожидаемая полезность с точки зрения террористов	Узел полезности	EU_t	Возможные значения определены в таблице 3

Узел 1 «Сценарий атаки» является узлом решения. Значения случайной переменной, определяющей его состояния выбирается террористами из трех возможных состояний: Сценарий 1, Сценарий 2 или Сценарий 3.

Узлы 2-10 относятся к типу случайных узлов сети. Состояние корневых узлов сети задается априорным распределением вероятностей. Для данной сети единственным корневым узлом является узел 2 «Наличие поддержки международных террористических организаций». Эта случайная переменная задается распределением: состояние «Да, есть поддержка» - 75%, состояние «Нет поддержки» - 25%.

Состояния каждого из некорневых узлов задаются таблицей условных вероятностей при различных состояниях его родителей $P(x_i \mid \pi_i)$: В частности состояние Узла 6. «Способность террористической организации спланировать атаку» определяется таблицей условных вероятностей (табл.2). Данные в таблице выбираются на основе экспертных оценок, имеющейся статистической информации или аналитических выкладок.

Таблица 2

Таблица условных вероятностей состояний Узла 6, в зависимости от состояний его предков (узлов 1 и 4)

1.Сценарий атаки - S_i	**Сценарий 1** ($S = s_1$)		**Сценарий 2** ($S = s_2$)		**Сценарий 3** ($S = s_3$)	
6. Способность спланировать атаку - SA	**Да** $SA = yes$	**Нет** $SA = no$	**Да** $SA = yes$	**Нет** $SA = no$	**Да** $SA = yes$	**Нет** $SA = no$
Да (способны спланировать атаку)	0.4	0	0.2	0	0.15	0
Нет (не способны спланировать атаку)	0.6	1	0.8	1	0.85	1

Аналогично составляются таблицы условных вероятностей для других случайных узлов модели.

Переменная 11 (EU_t) представлена на диаграмме узлом полезности. Значения задаются, исходя из того как аналитики антитеррористических сил, рассуждая за террористов, оценивают (с точки зрения террористов) ущерб, наносимый в случае реализации атаки рассматриваемого сценария, и затраты на организацию и осуществление указанной атаки: В рассматриваемом иллюстративном примере используются следующие числовые значения: Пусть рассматриваются два возможных состояния объекта: $V = v_0$ - объект – не поврежден, $V = v_1$ - объект поврежден. В случае если объект поврежден, ущерб, наносимый атаками, осуществленными по сценариям 1, 2,3 составляют соответственно: $U_t(s_1) = 5000$ *y.e.*, $U_t(s_2) = 20000$ *y.e.*, $U_t(s_3) = 15000$ *y.e.* Затраты на осуществление атак по сценариям 1,2 и 3 не зависят от того, был ли в результате атаки поврежден объект или нет, и составляют соответственно: $Z_t(s_1) = 100$ *y.e.*, $Z_t(s_2) = 400$ *y.e.*, $Z_t(s_3) = 150$ *y.e.*[2]

Тогда, согласно выражению (4), матрица полезности для данной сети будет иметь вид:

$$Ut_t(s_i; v_j) = \begin{bmatrix} -100 & 4900 \\ -400 & 19600 \\ -150 & 14850 \end{bmatrix}$$

Эту матрицу удобнее задавать в табличном виде, как это принято в байесовых сетях:

[2] Нижний индекс *t* означает, что оценка осуществляется с точки зрения террористов.

Таблица 3.

Таблица значений полезности, с точки зрения террористов при различных вариантах состояний «родителей» узла полезности

Сценарий атаки	**Сценарий 1 ($S = s_1$)**		**Сценарий 2($S = s_2$)**		**Сценарий 3 ($S = s_3$)**	
Состояние объекта	Объект не поврежден ($V = v_0$)	Объект поврежден ($V = v_1$)	Объект не поврежден ($V = v_0$)	Объект поврежден ($V = v_1$)	Объект не поврежден ($V = v_0$)	Объект поврежден ($V = v_1$)
Значение полезности, $Ut_t(s_i; v_i)$, у.е.	-100	4900	-400	19600	-150	14850

Пусть террористами принято решение об организации атаки по сценарию 1. Диаграмма влияния для этого случая представлена на рис. 2. При этом вероятность того, что атака окажется успешной (т.е., что объект будет поврежден) составляет: $P_t(V = v_1 \mid S = s_1) = 18{,}30\%$, а значение ожидаемой полезности равно $EU_t(s_1) = 815{,}16$ у.е.

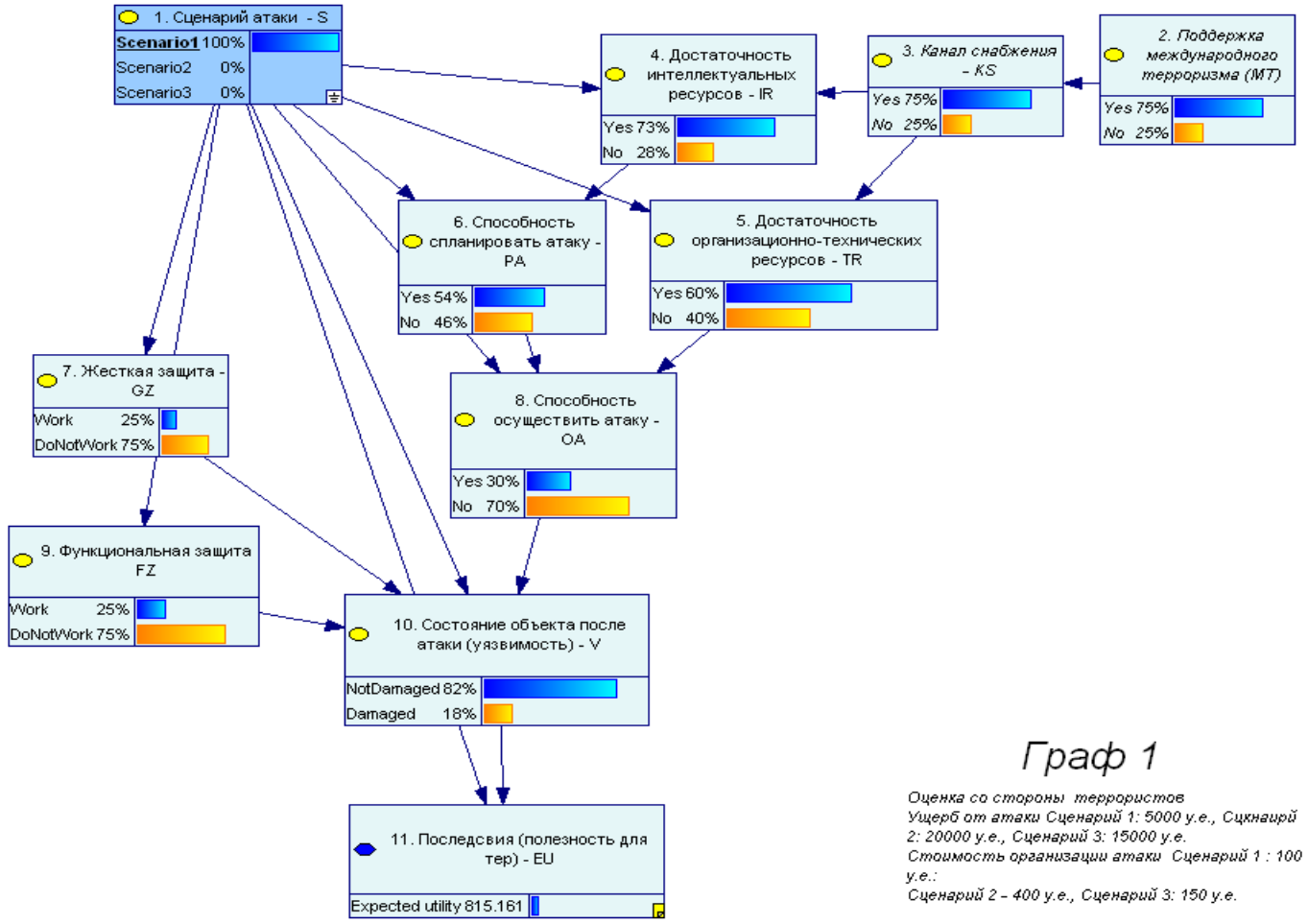

Рис. 2. Диаграмма влияния с точки зрения террористов при реализации атаки по Сценарию 1. Представленная диаграмма является частью графического интерфейса программного комплекса GeNie 2.0. Использование английских слов для описания состояний узлов модели является вынужденным, поскольку диктуется требованиями используемого программного комплекса. В данной и последующих диаграммах используются следующие английские обозначения: Expected utility - ожидаемая полезность, scenario –сценарий атаки, yes- да, no –нет, work – действует, DoNotWork – не действует, NotDamaged –не поврежден, Damaged –поврежден.

В случае организации атаки по Сценарию 2 вероятность повреждения объекта равна $P_t(V = v_1 \mid S = s_2) = 8{,}30\%$, а ожидаемая полезность составляет $EU_t(s_2)$ =1260,84 у.е. В случае атаки по Сценарию 3 $P_t(V = v_1 \mid S = s_3)$ =1,89%, $EU_t(s_3)$ =134,71 у.е.

К достоинствам байесовых сетей следует отнести наличие алгоритмов, позволяющих уточнять значения вероятностей для состояний переменных модели после того, как появляются дополнительные сведения о состоянии отдельных узлов. Пусть, например, террористы получают достоверную информацию, что их канал снабжения работает устойчиво $(KS = Yes)$, и, что функциональная система защиты объекта – не действует $(FZ = DoNotWork)$. Тогда, в случае если выбран 1-ый сценарий атаки, сеть принимает вид представленный на рис. 3.

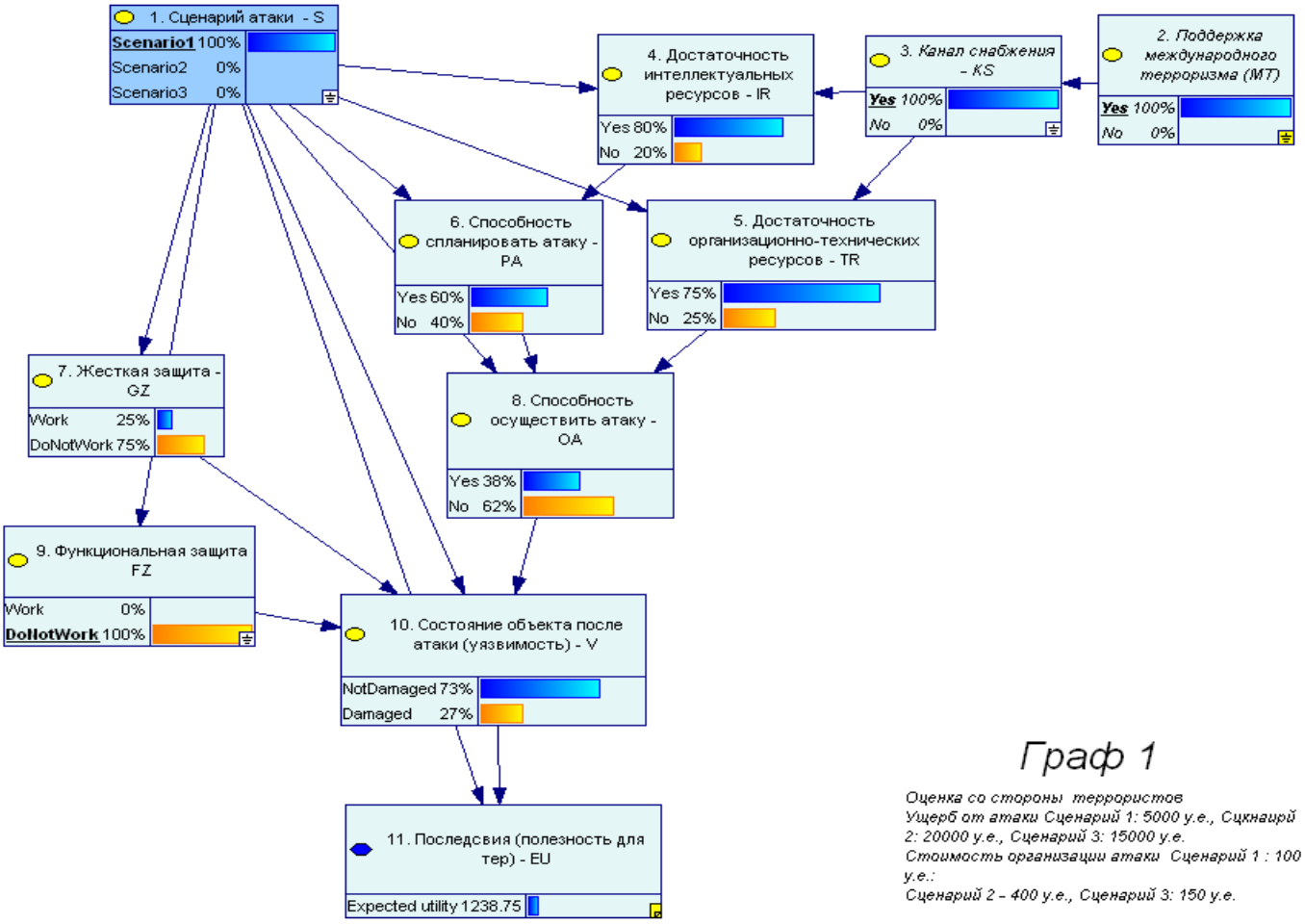

Рис. 3. Получение апостериорных оценок вероятностей состояний переменных системы.

Алгоритмы пересчета вероятностей позволяют найти апостериорные значения вероятности того, что в результате атаки объект будет поврежден $P_t^*(V = v_1 \mid S = s_1; KS = Yes; FZ = DoNotWork)$ =26,77%, а значение ожидаемой полезности $EU_t^*(s_1)$=1238.75 у.е. Полученные величины заметно отличаются от априорных оценок $P_t(V = v_1 \mid S = s_1) = 18{,}30\%$ и $EU_t(s_1) = 815{,}16$ у.е.

Для того чтобы аналитики антитеррористических сил могли оценить вероятность осуществления террористами определенного сценария атаки вводятся следующие допущения[3]:
1) Рассмотренные сценарии атаки $(s_1; s_2; \ldots, s_n)$ образуют полную группу взаимоисключающих событий (т.е. рассмотренный перечень возможных сценариев атак является исчерпывающим, и у террористов хватает ресурсов на осуществление только одного сценария атаки).
2) Вероятность осуществления атаки по i - сценарию определяется выражением (6).

[3] Pate-Cornell E. Probabilistic Modeling of Terrorist Threats: A Systems Analysis Approach to Setting Priorities Among Countermeasures. Military Operations Research, Vol. 7, No 4, pp. 5-20 December 2002.

$$P_t(S=s_i)=\frac{EU_t(s_i)}{\sum_{k=1}^{n}EU_t(s_k)} \qquad (6)$$

Таким образом, используя выражение (6), в результате анализа Графа 1 трехсторонней модели аналитик анитеррористических сил может оценить вероятности реализации различных сценариев атаки: $P_t(S=s_1)=36{,}87\%$; $P_t(S=s_2)=57{,}03\%$; $P_t(S=s_3)=6{,}09\%$.

4.2 Построение диаграммы влияния, характеризующей ситуацию с точки зрения администрации объекта, подвергающегося атаке террористов.

Далее рассматривается Граф 2 (рис. 4) интегральной модели. Здесь узел 1 -сценарий атаки становится случайным узлом, состояние которого описывается распределением (6), полученным в результате анализа графа 1 модели.

В Графе 2 появляются дополнительные узлы:

Узел 7. Наличие информации от спецслужб о планировании атаки (IP), который имеет два возможных состояния - Да/нет

Узел 8. Наличие информации от спецслужб об организации атаки (IO), также имеющий два возможных состояния: - Да/нет

Узел решения 14 определяет три варианта мер по противодействию террористической атаке:

Вариант 1. $(D=d_1)$ Не предпринимать никаких мер

Вариант 2. $(D=d_2)$ Действия по нарушению канала снабжения террористов

Вариант 3. $(D=d_3)$ Действия по организации охранной системы защиты.

Узел 15 (NS)– определяет нарушение канала снабжения.

Узел 16 (OZ) – определяет организацию охраной системы защиты.

Узел полезности 13 (EU) характеризуется следующей функцией полезности: Значения функции полезности задаются исходя из сделанных аналитиками антитеррористических сил оценок ущерба, который наносится государству атаками, осуществленными по различным сценариям и оценок затрат на осуществление защитных мероприятий.

Ущерб, наносимый атаками, осуществленными по сценариям 1, 2, 3 составляет $U_a(s_1)=5000\ y.e.$, $U_a(s_2)=20000\ y.e.$, $U_a(s_3)=15000\ y.e.$ Нижний индекс «a» означает, что оценка осуществляется с точки зрения администрации объекта.[4] Затраты на осуществление защитных мероприятий 1, 2 и 3 составляют: $Z_a(d_1)=0$, $Z_{at}(d_2)=300\ y.e.$, $Z_a(d_3)=200\ y.e.$ Тогда значение функции полезности для узла 13. задается таблицей 5. Фигурирующие в таблице отрицательные величины (значения, так называемой, отрицательной полезности), подсчитываются как сумма ущербов при различных сценариях атаки и затрат, на реализацию различных антитеррористических мер)

Таблица 5.

Таблица значений полезности, с точки зрения администрации объекта при различных вариантах состояний «родителей» узла полезности

Сценарий атаки, s_i	**Сценарий 1 ($S=s_1$)**		**Сценарий 2($S=s_2$)**		**Сценарий 3 ($S=s_3$)**	
Состояние объекта v_j	Объект не поврежден $(V=v_0)$	Объект поврежден $(V=v_1)$	Объект не поврежден $(V=v_0)$	Объект поврежден $(V=v_1)$	Объект не поврежден $(V=v_0)$	Объект поврежден $(V=v_1)$

[4] Оценка ущерба от террористической атаки с точки зрения администрации может заметно отличаться от оценки ущерба, сделанной террористами $U_a(s_i)\neq U_t(s_i)$. В частности, могут учитываться вторичные и каскадные ущербы, а также ущербы с отложенным эффектом. Кроме того функции полезности террористов и антитеррористических сил - существенно отличаются. Однако в рассматриваемом примере эти величины считаются равными.

Вариант защитных мер, $D = d_k$	Никаких мер, d_1	Наруш. канала снабжения, d_2	Охранная защита,d_3	Никаких мер, d_1	Наруш. канала снабжения, d_2	Охранная защита,d_3	Никаких мер, d_1	Наруш. канала снабжения, d_2	Охранная защита,d_3	Никаких мер, d_1	Наруш. канала снабжения, d_2	Охранная защита,d_3	Никаких мер, d_1	Наруш. канала снабжения, d_2	Охранная защита,d_3	Никаких мер, d_1	Наруш. канала снабжения, d_2	Охранная защита,d_3
Значение полезности, $Ut_a(s_i; v_j; d_k)$,у.е	0	-300	-200	-5000	-5300	-5200	0	-300	-200	-20000	-20300	-20200	0	-300	-200	-15000	-15300	15200

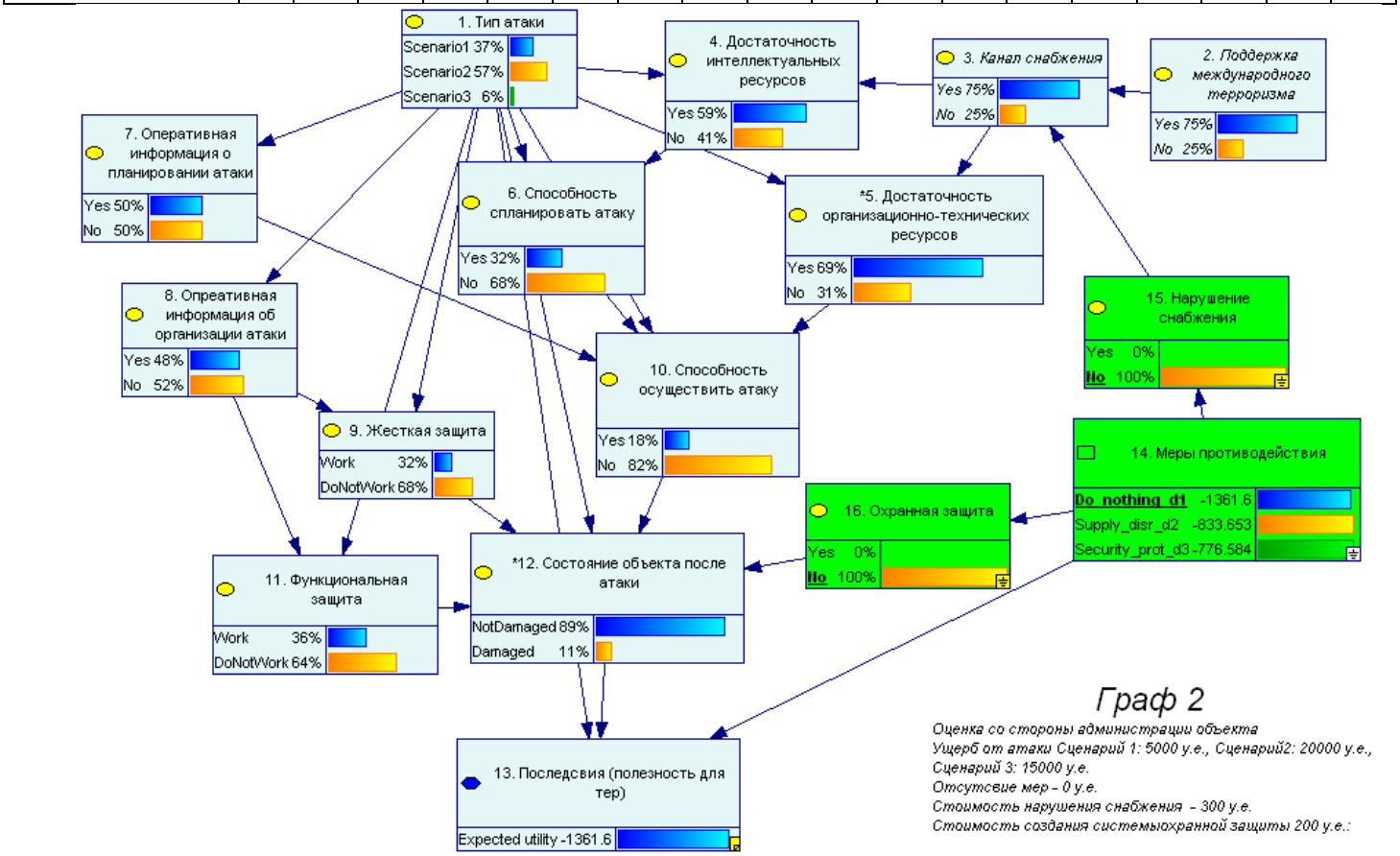

Рис. 4. Диаграмма влияния для варианта решения, при котором защитные меры не предпринимаются. (Обозначения: Do_nothing_d1 – без защитных мер, Supply_disr_d2 – нарушение канала снабжения, Security_prot_d3 – создание системы охранной защиты)

В случае принятия варианта решения $D = d_1$: Вероятность успеха атаки будет равняться $P(V = v_1 \mid D = d_1)$=11,18%; ожидаемая полезность $EU(d_2) = -1361{,}6$ у.е.

Диаграмма влияния для варианта решения $D = d_2$ (нарушение канала снабжения) представлена на рис. 5.

В этом случае вероятность успеха атаки равна $P_a(V = v_1 \mid D = d_2) = 4{,}30\%$, а ожидаемая полезность: $EU_a(d_2) = -833{,}65$ у.е.

Аналогично, построив диаграмму влияния для варианта решения $D = d_3$, находим вероятность повреждения объекта: $P_{at}(V = v_1 \mid D = d_3) = 4{,}46\%$, ожидаемая полезность $EU_a(d_3) = -776{,}58$ у.е.

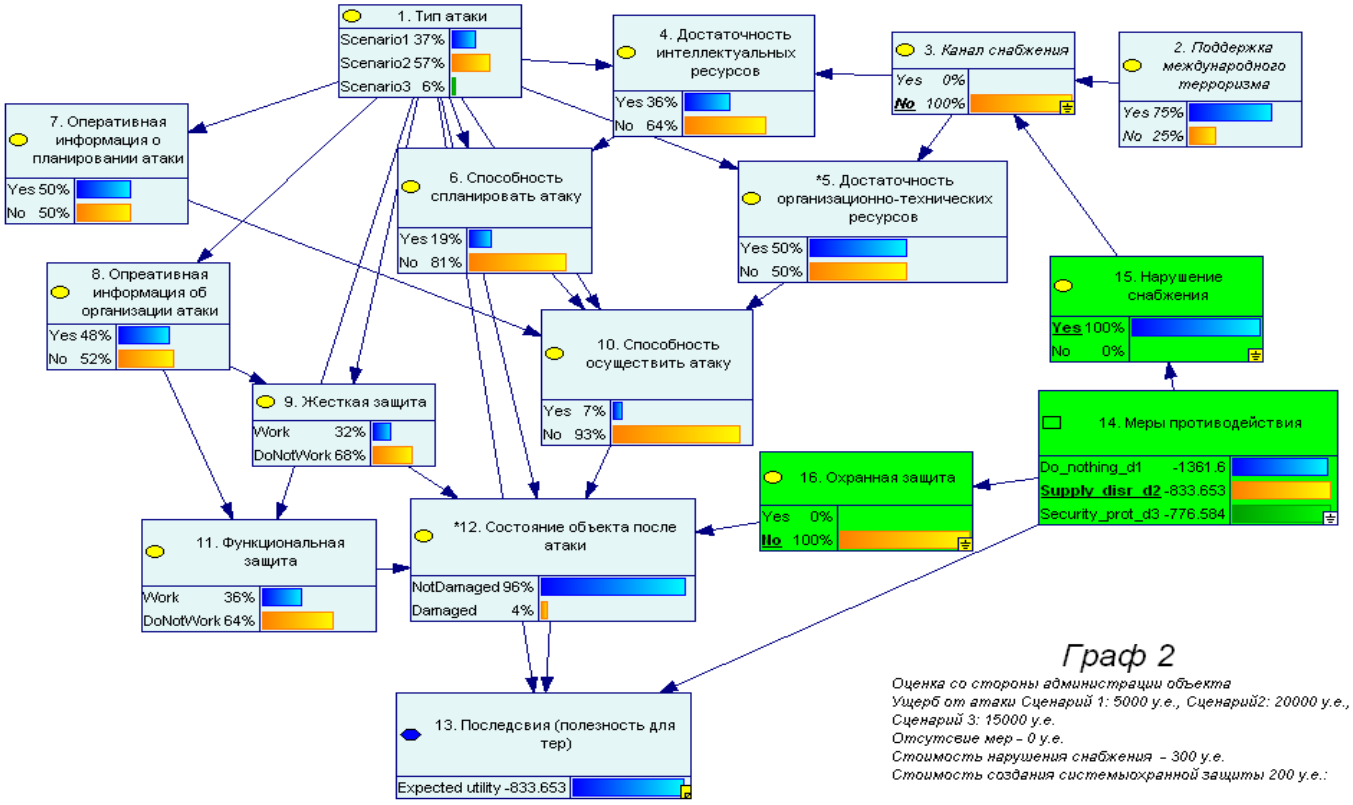

Рис. 5. Диаграмма влияния для варианта решения $D = d_2$.

Таким образом, наиболее эффективным является третий вариант защитных мероприятий администрации объекта, обеспечивающий минимальное (по модулю) значение отрицательной полезности $EU_a(d_3) = -776{,}58$ у.е., который и должен быть рекомендован в качестве наиболее эффективного способа снижения террористического риска для рассматриваемого объекта.

4.3 Построение диаграммы влияния, характеризующей ситуацию с точки муниципальных властей района, в котором расположен рассматриваемый объект (граф 3).

В представленный граф вводятся следующие узлы:

Узел 1. Сценарий атаки – определяется также как и одноименный узел графа 2.

Узел 2. Состояние объекта в после атаки. Узел имеет два состояния: объект не поврежден ($V = v_0$)и объект поврежден ($V = v_1$). Вероятности нахождения узла в указанных состояниях определяются для каждого из сценариев атак с помощью Графа 2. Полагая узел 14 Графа 2, находящимся в состоянии $D = d_3$и присваивая переменной сценария атаки Sпоочередно значения $s_1, s_2, \ldots, s_n$, вычисляются вероятности нахождения объекта в каждом из двух возможных состояний: состоянии «объект не поврежден» ($V = v_0$) и состоянии «объект поврежден» ($V = v_1$). Результаты расчета представлены в таблице 6.

Таблица 6.

Вероятности нахождения объекта в неповрежденном и поврежденном состояниях при различных сценариях атаки.

Сценарий атаки, S_i	**Сценарий 1** ($S = s_1$)	**Сценарий 2** ($S = s_2$)	**Сценарий 3** ($S = s_3$)
Объект не поврежден $P(V = v_0 \mid S = s_i; D = d_2)$	0.92	0.974	0.985
Объект поврежден $P(V = v_1 \mid S = s_i; D = d_2)$	0.08	0.026	0.015

Узел 3. Является узлом решения и описывает варианты решений, принимаемых муниципальными властями с целью минимизации ущерба от террористической атаки для населения и объектов социальной инфраструктуры, которые могут оказаться в зоне поражения, в случае разрушения рассматриваемого объекта. Узел 3 определяет три варианта мер, принимаемых муниципальными властями, для противодействия террористической угрозе:

Вариант 1. $M = m_1$ не предпринимать никаких мер.

Вариант 2. $M = m_1$ - действия по предупреждению паники (работа со СМИ и населением)

Вариант 3. $M = m_1$ - вынесение социально значимых объектов из зоны поражения при атаке.

Узел 4. Определяет реализацию решения о предупреждении паники

Узел 5. Определяет реализацию решений о вынесении социальной инфраструктуры из зоны поражения при террористической атаке.

Узел 6 определяет режим освещения террористической атаки средствами массовой информации (возможные состояния: ограниченный уровень информации и чрезмерный уровень информации).

Узел 7 определяет интегральный индекс психологического состояния населения, находящегося в зоне поражения при атаке (возможные состояния узла: спокойствие и паника).

Узел 8 определяет интегральную характеристику состояния зданий и объектов инфраструктуры, находящихся в зоне поражения при атаке (возможные значения: ограниченные повреждения и значительные повреждения)

Узел 9 определяет функцию полезности, значения которой представлены в таблице 7.

Таблица 7

Функция полезности действий муниципальных властей

Сценарий атаки S_i	Состояние соц. Инфраструктуры в зоне поражения, SI_j	Состояние населения, SN_k	Меры противодействия, M_l	Полезность для муниципальных властей $U_m(S_i, SI_jSN_k, M_l)$ у.е.
Сценарий 1, S_1	Не повреждена, SI_1	Спокойствие, SN_1	Никаких действий, m_1	0
Сценарий 1, S_1	Не повреждена, SI_1	Спокойствие, SN_1	Предотвращение паники, m_2	-300
Сценарий 1, S_1	Не повреждена, SI_1	Спокойствие, SN_1	Вынесение соц. инфр. из ЗП, m_3	-100
Сценарий 1, S_1	Не повреждена, SI_1	Паника, SN_2	Никаких действий, m_1	-3000
Сценарий 1, S_1	Не повреждена, SI_1	Паника, SN_2	Предотвращение паники, m_2	-3300
Сценарий 1, S_1	Не повреждена, SI_1	Паника, SN_2	Вынесение соц. инфр. из ЗП, m_3	-3100
Сценарий 1, S_1	Повреждена, SI_2	Спокойствие, SN_1	Никаких действий, m_1	-30000
Сценарий 1, S_1	Повреждена, SI_2	Спокойствие, SN_1	Предотвращение паники, m_2	-30300
Сценарий 1, S_1	Повреждена, SI_2	Спокойствие, SN_1	Вынесение соц. инфр. из ЗП, m_3	-30100
Сценарий 1, S_1	Повреждена, SI_2	Паника, SN_2	Никаких действий, m_1	-33000
Сценарий 1, S_1	Повреждена, SI_2	Паника, SN_2	Предотвращение паники, m_2	-33300
Сценарий 1, S_1	Повреждена, SI_2	Паника, SN_2	Вынесение соц. инфр. из ЗП, m_3	-33100
Сценарий 2, S_2	Не повреждена, SI_1	Спокойствие, SN_1	Никаких действий, m_1	0
Сценарий 2, S_2	Не повреждена, SI_1	Спокойствие, SN_1	Предотвращение паники, m_2	-300
Сценарий 2, S_2	Не повреждена, SI_1	Спокойствие, SN_1	Вынесение соц. инфр. из ЗП, m_3	-100
Сценарий 2, S_2	Не повреждена, SI_1	Паника, SN_2	Никаких действий, m_1	-3000
Сценарий 2, S_2	Не повреждена, SI_1	Паника, SN_2	Предотвращение паники, m_2	-3300
Сценарий 2, S_2	Не повреждена, SI_1	Паника, SN_2	Вынесение соц. инфр. из ЗП, m_3	-3100
Сценарий 2, S_2	Повреждена, SI_2	Спокойствие, SN_1	Никаких действий, m_1	-30000

Сценарий 2, S_2	Повреждена, SI_2	Спокойствие, SN_1	Предотвращение паники, m_2	-30300
Сценарий 2, S_2	Повреждена, SI_2	Спокойствие, SN_1	Вынесение соц. инфр. из ЗП, m_3	-30100
Сценарий 2, S_2	Повреждена, SI_2	Паника, SN_2	Никаких действий, m_1	-33000
Сценарий 2, S_2	Повреждена, SI_2	Паника, SN_2	Предотвращение паники, m_2	-33300
Сценарий 2, S_2	Повреждена, SI_2	Паника, SN_2	Вынесение соц. инфр. из ЗП, m_3	-33100
Сценарий 3, S_3	Не повреждена, SI_1	Спокойствие, SN_1	Никаких действий, m_1	0
Сценарий 3, S_3	Не повреждена, SI_1	Спокойствие, SN_1	Предотвращение паники, m_2	-300
Сценарий 3, S_3	Не повреждена, SI_1	Спокойствие, SN_1	Вынесение соц. инфр. из ЗП, m_3	-100
Сценарий 3, S_3	Не повреждена, SI_1	Паника, SN_2	Никаких действий, m_1	-3000
Сценарий 3, S_3	Не повреждена, SI_1	Паника, SN_2	Предотвращение паники, m_2	-3300
Сценарий 3, S_3	Не повреждена, SI_1	Паника, SN_2	Вынесение соц. инфр. из ЗП, m_3	-3100
Сценарий 3, S_3	Повреждена, SI_2	Спокойствие, SN_1	Никаких действий, m_1	-40000
Сценарий 3, S_3	Повреждена, SI_2	Спокойствие, SN_1	Предотвращение паники, m_2	-40300
Сценарий 3, S_3	Повреждена, SI_2	Спокойствие, SN_1	Вынесение соц. инфр. из ЗП, m_3	-40100
Сценарий 3, S_3	Повреждена, SI_2	Паника, SN_2	Никаких действий, m_1	-43000
Сценарий 3, S_3	Повреждена, SI_2	Паника, SN_2	Предотвращение паники, m_2	-43300
Сценарий 3, S_3	Повреждена, SI_2	Паника, SN_2	Вынесение соц. инфр. из ЗП, m_3	-43100

Диаграмма влияния для варианта мер муниципальных властей по снижению последствий $M = m_1$ (никаких действий) принимает вид, представленный на рисунке 6. В этом случае вероятность разрушения социальной инфраструктуры составляет $P(SI = Damaged \mid M = m_1) = 3{,}54\%$, вероятность паники среди населения - $P(SN = Panica \mid M = m_1) = 64{,}37\%$, а ожидаемая полезность для муниципальных властей составляет $EU_m(M = m_1) = -3001{,}4$ у.е.

В случае второго варианта действия по снижению последствий ($M = m_2$ предотвращение паники среди населения) вероятность разрушения социальной инфраструктуры по прежнему составляет $P(SI = Damaged \mid M = m_2) = 3{,}54\%$, вероятность паники снижается до - $P(SN = Panica \mid M = m_2) = 15{,}08\%$, а ожидаемая полезность для муниципальных властей составляет $EU_m(M = m_2) = -1822{,}7$ у.е.

Если будет избран третий вариант действий ($M = m_3$ - вынесение социальной инфраструктуры из зоны поражения при атаке на рассматриваемый объект), то будут получены следующие значения выходных параметров модели: вероятность разрушения социальной инфраструктуры $P(SI = Damaged \mid M = m_3) = 0$, вероятность паники - $P(SN = Panica \mid M = m_3) = 64{,}37\%$, а ожидаемая полезность для муниципальных властей составляет $EU_m(M = m_2) = -2031{,}22$ у.е.

Таким образом, наиболее эффективным следует признать второй вариант действий муниципальных властей по снижению ущерба от возможной атаки на рассматриваемый объект.

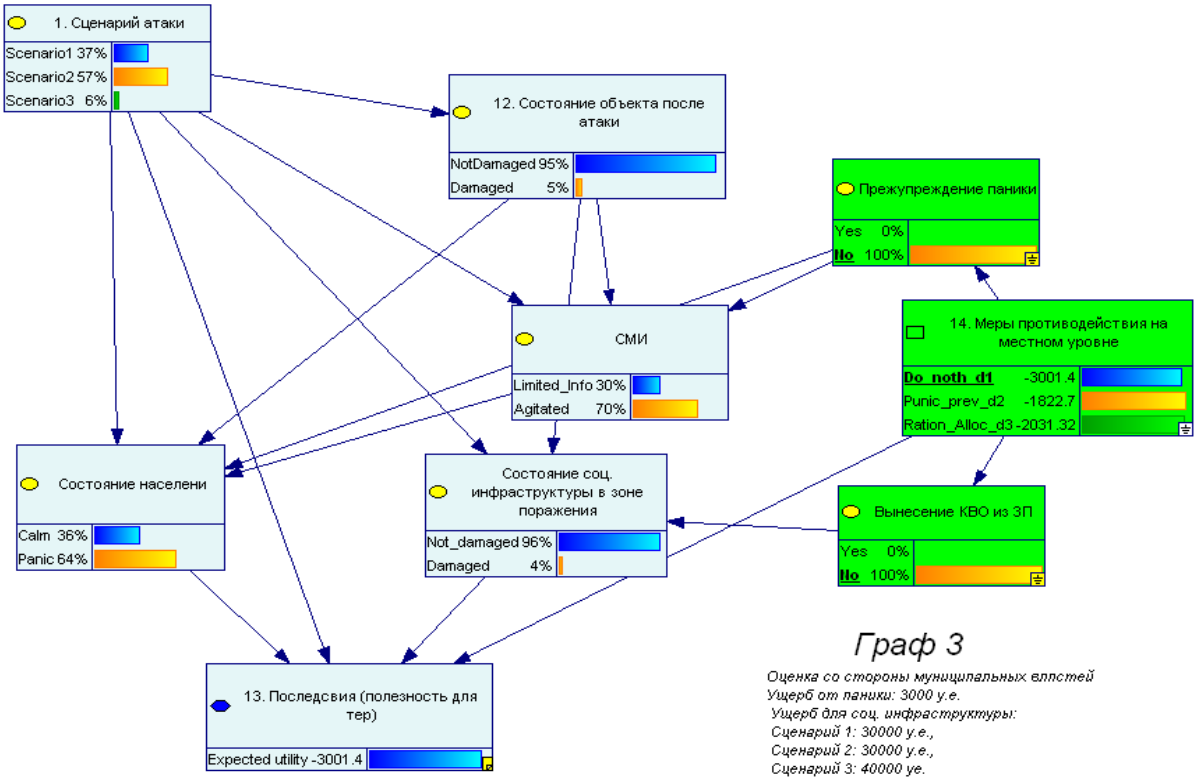

Рис. 6. Диаграмма влияния, для варианта решения муниципальных властей

Обозначения: Do_nothing_d1 - не предпринимать никаких мер; Punic_prev_d2 - действия по предупреждению паники; Rational_aloc_d3 - вынесение социально значимых объектов из зоны поражения при атаке;Limited_Info – ограниченная информация об атаке со стороны .СМИ, Agitated –возбуждение ажиотажа средствами массовой информации, Calm – спокойное состояние население, Panic – паника среди населения.

Представленная трехсторонняя модель оценки и управления террористическим риском является статической и соответствует некоторому моменту времени t_k. На следующем этапе игровой процедуры варианты защитных мер (d_3 и m_2), предпринимаемые соответственно администрацией объекта и муниципальными властями, могут быть включены в граф 1 модели. Тем самым террористы отреагируют на действия антитеррористических сил и смогут найти наиболее эффективный сценарий атаки с учетом изменений в системе защиты объекта и прилегающей к нему территории. Вероятности реализации вариантов защитных мер d_j и m_l могут оцениваться террористами исходя из следующих соотношений:

$$P_a(D=d_j)=\frac{EU_a(d_j)}{\sum_{g=1}^{3}EU_a(d_g)},\ k=1,2,3$$

$$P_m(M=m_l)=\frac{EU_m(m_l)}{\sum_{f=1}^{3}EU_m(m_f)},\ l=1,2,3 \qquad (7)$$

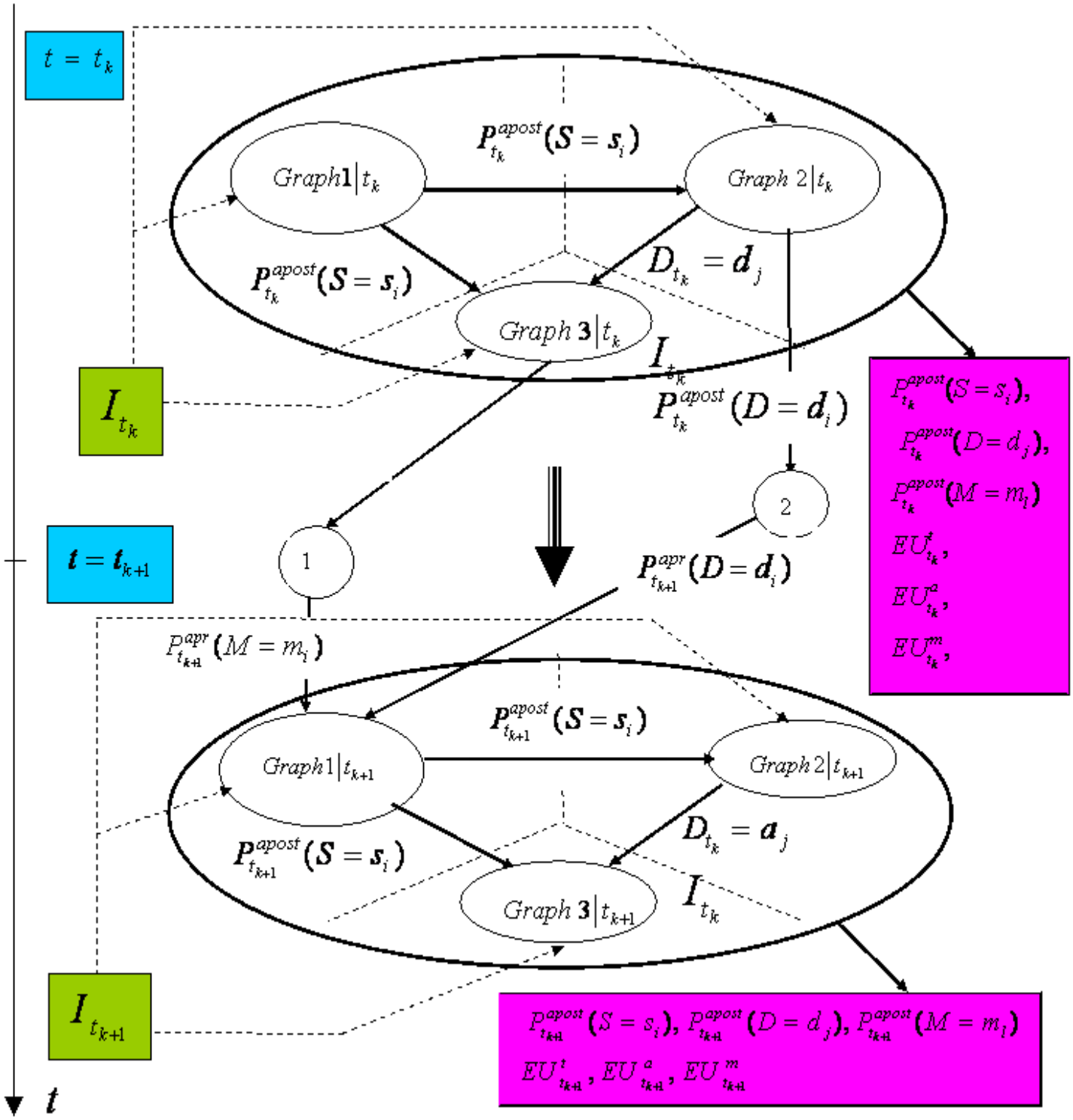

Рис.7. Фрагмент динамической модели оценки террористического риска.

Таким образом, учитывая динамические изменения рассматриваемой системы, трехсторонняя модель оценки террористического риска в момент времени $t_{k+1} = t_k + \Delta t$ будет несколько отличаться от момента времени t_k (Рис. 7). В граф 1 могут быть включены узлы графов 2 и 3, описывающие варианты защитных мероприятий администрации объекта и муниципальных властей: (узлы 14, 15,16 Графа 2 и узлы 3, 4, 5 Графа 3). При этом указанные узлы становятся случайными. Таблицы распределения вероятностей для этих узлов формируются на основе выражений (7), используя апостериорные оценки вероятностей при $t = t_k$ как априорные оценки для момента $t = t_{k+1}$:

$$P^{apr}_{t_{k+1}}(D = d_i) = P^{apost}_{t_k}(D = d_j)$$
$$P^{apr}_{t_{k+1}}(M = m_i) = P^{apost}_{t_k}(M = m_i) \qquad (8)$$

Кроме того, с учетом вновь поступающей информации может быть скорректирована не только структура диаграмм влияния, отражающая качественную конфигурацию модели, но и таблицы условных вероятностей, отражающие вероятностные связи между переменными модели. Условно это представлено с помощью блоков I_{t_k} и $I_{t_{k+1}}$, которые отражают совокупность имеющейся информации (статистических данных, оперативных сведений и аналитических умозаключений) на моменты времени t_k и t_{k+1}. При переходе к следующему дискретному значению времени должна быть учтена дополнительная информация о состоянии некоторых переменных модели (см. рис.3). Это позволит получить для момента времени t_{k+1} апостериорные оценки вероятностей и таким образом осуществлять дискретный мониторинг ситуации.

Каждый узел предложенной интегральной модели представляет собой результат анализа (моделирования, экспертной оценки) отдельной подзадачи, относящейся к определенной научной дисциплине или сфере деятельности, и решаемой специалистами соответствующего профиля. В число таких подзадач входят: оценка спектра и интенсивности террористических угроз для рассматриваемого объекта, анализ организационно-технического и интеллектуального потенциала террористической организации, ее целей и задач, анализ параметров уязвимости объекта по отношению к превалирующим угрозам, оценка эффективности систем защиты объекта и различных вариантов антитеррористических мероприятий. Особый интерес представляет задача, связанная с оценкой мотивационных установок, приоритетов и системы ценностей террористов, определяющих их функцию полезности, и задача по расчету ожидаемых ущербов от террористической атаки.

Представленная трехсторонняя модель является весьма упрощенной, таблицы условных вероятностей соответствующие, узлам графов составлены произвольно и не отражают ситуацию на реальных объектах. Также произвольно составлены таблицы функций полезности. Однако представленная модель позволяет описать принципиальный подход к оценке террористических рисков с учетом динамического взаимодействия террористических и антитеррористических сил, и может служить основой для принятия решений о целесообразности реализации тех или иных защитных мероприятий.

Литература.

1. К.В.Фролов, Н.А. Махутов, и др. Анализ риска и проблем безопасности. МГФ «Знание», 2006 г. Часть 1 - 639 стр., часть 2- 748 стр.

2. В.П.Петров, Д.О.Резников и др.Оценка террористического риска и принятие решений о целесообразности построения систем защиты от террористических воздействий. Проблемы безопасности и чрезвычайных ситуаций. 2007. №1, стр. 89-105.

3. Г.А. Поллак. Инструментальные средства разработки экспертных систем. Учебное пособие. Южноуральский государственный университет. Челябинск. Издательство ЮУРГУ.2003 г.

4. С.А. Терехов. Введение в байесовы сети. Научная сессия МИФИ. V Всероссийская научно-практическая конференция. Москва. 2003 г.

5. Терроризм. Снижение уязвимости и повышение ответных мер. Материалы Российско-американского семинара. «Вятка» 2004 г. 295 стр.

6. Charniak E. Bayesian Networks without Tears. AI Magazine, 12, 50-63

Граф 3

7. Jensen F. V.. An Introduction to Bayesian Networks. New York: Springer-Verlag. 1996.
8. Jensen F. V. Bayesian Networks and Decision Graphs (2001 ed.). New York: Springer. 2001.
9. Hausken K.. Probabilistic Risk Analysis and Game Theory. Risk Analysis, Vol 22, No1, 2002, pp. 17-27.
10. Howard R. and Matheson J. Influence Diagrams. Decision Analysis. Vol. 2, No. 3, September 2005, pp. 127–143
11. Kevin P. Murphy. Dynamic Bayesian Networks: Representation,Inference and Learning. PhD thesis, U.C. Berkeley, July 2002.
11. Linwood D. Hudson, Bryan S. Ware, Suzanne M. Mahoney. An Application of Bayesian Networks to Antiterrorism Risk Management for Military Planners.
13. Major J. "Advanced techniques for modeling terrorism risk". Journal of Risk Finance, 2002.
14. McCain R., 'Game Theory:An Introductory Sketch (Available as http://william-king.www.drexel.edu/ top/eco/game/nash.html)
15. Pate-Cornell E. Probabilistic Modeling of Terrorist Threats: A Systems Analysis Approach to Setting Priorities Among Countermeasures. Military Operations Research, Vol. 7, No 4, pp. 5-20 December 2002.
16. Pate-Cornell E. Risks of Terrorist Attacks of Terrorist Attacks. Presentation at Terrorism Risk Analysis Symposium. USC. 2005
17. Pearl J. 1988. Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference. Morgan Kaufmann, San Mateo, California. 1988.
19. Sandler T., Arce D. Terrorism and Game Theory. Simulation & Gaming. Vol. 34 (3) 2003.
20. Von Neumann, J. and Morgenstern, O. (1944) Theory of Games and Economic Behavior, Princeton University Press.
21.Weaver R., et. al. (2001) Modeling and Simulating Terrorist Decision-making: A "Performance Moderator Function" Approach to Generating Virtual Opponents, Philadelphia: University of Pennsylvania. (Available as http:// www.seas.upenn.edu:8080/~barryg/terrist.pdf)
22. Woo G. "Quantitative Terrorism Risk Assessment." The Journal of Risk Finance, Vol.4, No 1 pp 15-24.
23. Woo G., "Quantifying Insurance Terrorism Risk," Risk Management. Solutions, Inc. To appear in Alternative Risk Strategies, M. Lane, ed., Risk Publications Ltd. (2002)
24. Terrorism. Reducing Vulnerabilities and Improving Responses. U.S.-Russian workshop proceedings. The National Academies Press. Washington, D.C. 2004.
25. K. Frolov, G.Baecher. "Protection of Civilian Infrastructure from Acts of Terrorism". Springer. P.O. Box 17, 3300 AA Dordrecht, The Netherlands. 2006. 252 p