УДК 658.314.7:330.115

© Бухарин С.Н., Цыганов В.В., Бочкарева Ю.Г.
Bucharin S., Tsyganov V., Bochkareva Y.

СИТУАЦИОННЫЙ АНАЛИЗ В ИНФОРМАЦИОННОЙ ОПЕРАЦИИ

SITUATION ANALYSIS IN INFORMATION OPERATION

Аннотация. *Рассмотрены основные положения анализа обстановки, в которой проводится информационная операция (кратко – ситуационного анализа). Он необходим для прогнозирования — важнейшей процедуры базового механизма проведения информационной операции. Охарактеризованы критерии достижения её дуальной цели (декларируемой и истинной). Задача информационной операции связана с минимизацией разностей между фактически достигнутыми показателями и нормативными (целевыми) их значениями. Эффективность (степень достижения дуальной цели) информационной операции зависит от контролируемых и неконтролируемых факторов. Ситуационный анализ направлен на уменьшение неопределенности этих факторов. Количественный анализ рисков предполагает оценки вероятности инцидентов и связанных с ними потерь. Такие оценки могут быть получены путем анализа сетей событий и определения их условных вероятностей экспертными и статистическими методами.*

Annotation. *Considered the backgrounds of the analysis of the situation in which the information operation is held (briefly - situational analysis). It is necessary for prediction - the major underlying procedure of information operation mechanism. Criteria to achieve its dual goal (the declared and true goal) are characterized. Problem of information operations associated with the minimization of the differences between the actual performance achieved and their normative (target) values. Effectiveness (the degree of achievement of the dual goal) information operation depends on controllable and uncontrollable factors of information impact. Situational analysis aimed at reducing the uncertainty of these factors. Qualitative risk analysis involves the identification of possible threats and losses, identifying their causes and effects. Quantitative risk analysis involves estimating the probability of incidents and associated losses. Such estimates can be obtained by analyzing network events and determine their conditional probabilities by means of expert and statistical methods.*

Ключевые слова. *Информация, операция, анализ, ситуация, цель, риск, воздействие, прогнозирование, оценка, фактор, вероятность, ущерб.*

Key words. *Information, operation, analysis, situation, goal, risk, impact, prediction, evaluation, factor, probability, damage.*

Процесс планирования и принятия решений при организации и проведении информационной операции начинается с анализа внешних и внутренних условий, обстановки, в которой она будет протекать (кратко - ситуационного анализа [1]). Ситуационный анализ лежит в основе процедуры прогнозирования — важнейшего элемента базовой модели организации информационного противоборства [2]. Ситуационный анализ основывается на системном подходе, исследовании операций, управленческом опыте. Он включает высокие гуманитарные технологии [3], используемые для исследования мотивов, поведения и реакций заинтересованных лиц на информационные воздействия.

1. Цели информационной операции

Ситуационный анализ подчинен целям информационной операции. Цель — это идеальное мысленное предвосхищение результата деятельности. В качестве со-

Бухарин Сергей Николаевич – кандидат физико-математических наук, старший научный сотрудник, ИПУ РАН, тел. +7(495) 580-48-80;
Цыганов Владимир Викторович – доктор технических наук, профессор, главный научный сотрудник, Институт проблем управления им. В.А.Трапезникова РАН, тел. (495)334-91-91;
Бочкарева Юлия Геннадьевна – кандидат технических наук, доцент, Российский государственный университет инновационных технологий и предпринимательства, Пензенский филиал.

Bucharin Sergey – the candidate of physical and mathematical sciences, the senior research scientist, IPM RAS, tel. +7(495) 580-48-80;
Tsyganov Vladimir – doktor of engineering sciences, chief researcher of V.A. Trapeznikov Institute of control sciences Russian academy of sciences, tel.(495)334-91-91;
Bochkareva Julia – candidate of technical sciences, associate professor, Russian state university in Penza.

знательного мотива цель направляет и регулирует подготовку и проведение информационной операции. Цели связаны с ценностями: в бизнесе — это овладение капиталом, в политике — властью [4].

Цели делят на качественные и количественные. Качественная цель может быть либо достигнута, либо нет. В информационной операции она связана с приобретением капитала и власти и имеет две градации: «приобрел» или «не приобрел». Однако качественный характер такой цели часто условен. Как правило, известны или определяются количественные показатели, необходимые для достижения цели. Например, для победы в первом туре выборов политику необходимо набрать 50 % и один голос. Количественная цель информационного противоборства определяется степенью достижения наилучшего возможного значения показателя.

Рассмотрим количественные цели в базовой модели организации информационной операции [2]. Выход объекта информационного воздействия (кратко – объекта) в периоде t характеризуется показателем y_t (например, его доходами или убытками), причем $\xi_t \le y_t \le P_t$, где P_t — максимальный показатель выхода объекта (его потенциал); ξ_t — минимальный показатель его выхода (возможности объекта), $t = 0,1,...$.

При развитии полезного объекта, количественная цель связана с минимизацией разности значений потенциала и реально достигнутого показателя y_t

$$\Delta_t = P_t - y_t \to \min. \qquad (1)$$

Например, в информационной операции, направленной на продвижение продукта на рынок (или кандидата на избрание), потенциал P_t — максимально возможное количество продаж (или число голосов на выборах); y_t — фактическое количество продаж (или число полученных голосов на выборах).

При подавлении вредного объекта количественная цель в информационной операции связана с минимизацией разности реально достигнутого показателя y_t и возможности объекта ξ_t

$$\delta_t = y_t - \xi_t \to \min, \qquad (2)$$

Для достижения количественной цели информационного противоборства, из множества возможных стратегий необходимо выбрать стратегии, обеспечивающие минимум критерия (1) или (2).

В информационных войнах часто используют дуальную цель. Суть её в следующем: объект декларирует одну цель, а преследует другую. Со времен античных демократий и крестовых походов информационные войны, направленные на «счастье для народа», приводят к благополучию для «избранных».

Дуализм цели информационной операции можно формализовать следующим образом:

$$J_1\left(\bar{R}\right) \underset{\bar{R}}{\to} \max;\ J_2\left(\bar{R}\right) \underset{\bar{R}}{\to} \max, \qquad (3)$$

где J_1 и J_2 — критерии достижения декларативной и истинной целей, соответственно; $\bar{R}$ — вектор ресурсов размерности n, $\bar{R} = (r_1, r_2, ..., r_n)$ где $r_1, r_2, ..., r_n$ — человеческие, материально-технические, административные и прочие ресурсы общим числом n. Предположим, что каждый из этих n ресурсов r_i является монотонно возрастающей функцией соответствующего финансового ресурса x_i

$$\bar{R} = \{r_1\left(x_1\right), r_2\left(x_2\right), ..., r_n\left(x_n\right)\}; \qquad (4)$$

$$x_1 + x_2 + ... + x_n \le X_0, \qquad (5)$$

где X_0 — финансовый ресурс, выделенный на реализацию проекта (бюджет). Решением задачи (3) – (5) является множество распределений бюджета, оптимальных по Парето по критериям $J_1\left(\bar{R}\right)$ и $J_2\left(\bar{R}\right)$. Это решение характерно для легальной истинной цели, связанной с денежным вознаграждением, карьерным ростом, качеством труда и т. п. Добиваясь ее, объект расходует бюджет (5), действуя в рамках закона.

Нелегальная цель связана с нарушением закона. Например, в условиях коррупции она сопряжена с личным обогащением объекта, которому доверено исполнение или контроль проекта. Это обогащение основано на присвоении финансовых ресурсов проекта через криминальные схемы.

Предположим, что коррумпированный объект направляет на реализацию проекта средства бюджета в размере X_1, незаконно присваивая остальные средства X_2. Тогда сумма затрат из бюджета

$$X_0 = X_1 + X_2. \qquad (6)$$

В этом случае достижение декларируемой и истинной нелегальной цели связано общностью бюджета, выделенного на реализацию проекта. «Дуализм» декларируемой и нелегальной истинной цели можно формализовать следующим образом:

$$J_1\left(\bar{R}(x)\right) \underset{\bar{R}}{\to} \max;\ x \le X_1;\ X_2 \underset{\bar{R}}{\to} \max, \qquad (7)$$

где J_1 и X_2 — критерии достижения декларируемой и нелегальной истинной цели, соответственно; $\bar{R}$ — вектор ресурсов размерности n, удовлетворяющий (4),

$$x_1 + x_2 + ... + x_n \le X_1, \qquad (8)$$

где X_1 — финансовый ресурс, выделяемый коррумпированным объектом на реализацию проекта. Решением за-

дачи (6) – (8) является множество распределений бюджета, оптимальных, по Парето, по критериям $J_1(\bar{R})$ и X_2. Это решение характерно для нелегальной истинной цели, связанной с хищением средств из бюджета.

Предположим, что размер похищаемых средств X_2 ограничен: $X_2 \le X_{20}$. Это ограничение зависит от степени коррумпированности социально-экономической системы, от того, насколько далеко зашла «степень криминального согласия» в обществе. Обозначим через k вероятность разоблачения. Будем считать, что наказание за незаконные действия состоит в возврате похищенных средств X_2. Тогда ожидаемая величина $\langle X_2 \rangle$ потерь коррумпированного объекта равна $\langle X_2 \rangle = k X_2$. На практике вероятность разоблачения k уменьшается при передаче части похищенных средств контролирующим органам. Если же коррупция пронизывает всю структуру управления и распределения ресурсов, то риск коррумпированного объекта стремится к нулю $k X_2 \to 0$.

Казалось бы, увеличению размера похищаемых средств X_2 препятствует публично декларируемая цель. Однако это не так. Можно назвать примеры, когда цели публично декларировались, под них выделялись ресурсы, а затем все «спускалось на тормозах», о целях забывали, а деньги, выделенные на их достижение, пропадали. Эффект коррумпированных сделок достигается за счет уменьшения целевых ресурсов бюджета X_1. Это, в частности, приводит к вымыванию интеллектуальных ресурсов из экономики, незаинтересованности в создании научно-технических заделов и инноваций, внедрения новых технологий в экономику страны. Таким образом, декларируемые цели о создании инновационной экономики не реализуются.

2. Факторы обстановки

Критерий эффективности достижения цели информационной операции зависит от множества факторов. Исследование их влияния включает, в частности, определение сильных и слабых сторон субъекта и объектов информационных воздействий — компании, партии, заинтересованных лиц, их затруднений и возможностей. Фактор — это причина, движущая сила какого-либо процесса, явления, определяющая его характер или отдельные его черты.

Ситуационный анализ рассматривает факторы, к которым чувствительна задуманная информационная операция [1]. Следуя работе [5], её чувствительность e_f по отношению к определенному фактору f, измеряется отношением изменения критерия эффективности достижения ее цели ΔK к изменению значения этого фактора Δf. Если фактор принимает значения, принадлежащие отрезку числовой оси, а критерий эффективности является непрерывно дифференцируемой его функцией, то чувствительность e_f равна производной критерия по этому фактору K_f'. Если сам фактор является функцией некоторой переменной $f=f(x)$, то критерий эффективности является функционалом, определенным на множестве возможных функций этой переменной $K = K\left(f\left(x\right)\right)$, а чувствительность e_f равна отношению вариации δK функционала к вариации δf этой функции $e_f = \delta K / \delta f$. Наконец, чувствительность может быть оценена с помощью экспертов. Чувствительность может меняться со временем, и тогда факторы, которые не влияли на ход операции, могут стать определяющими.

Факторы, влияющие на успех информационной операции, принято классифицировать на контролируемые (управляемые) и неконтролируемые [1] (рис.1).

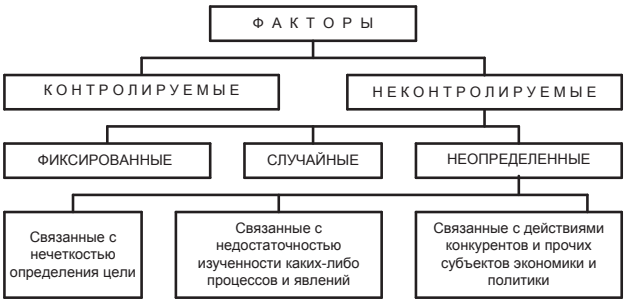

Рис. 1. Классификация факторов

Контролируемые факторы — это воздействия на объект, вырабатываемые субъектом информационного управления. Эти воздействия формируются на основе правил и процедур, устанавливаемых субъектом. К ним относятся процедуры прогнозирования, планирования, распределения ресурсов и стимулирования объекта. Совокупность этих процедур называется механизмом функционирования организационной системы, объединяющей субъект и объект информационного управления [2]. Отсутствие механизма функционирования превращает контролируемые факторы в неконтролируемые. Более того, при плохом менеджменте они могут оказаться под контролем конкурента.

К контролируемым факторам относятся ресурсы, которые находятся в распоряжении субъекта, проводящего операцию. Ими можно управлять с разной степенью эффективности. Субъекты информационного управления могут образовать коалицию и объединить ресурсы на основе общих интересов. В этом случае между участниками коалиции существует компромисс, отсутствует конфликт и конкуренция. Такие коалиции назы-

вают коалициями интересов. Для участия в информационных операциях их субъекты заключают коалиции действий. К ним относятся, например, картельные сговоры монополистов.

Неконтролируемые факторы — это воздействия на объект, не зависящие от субъекта информационного управления (рис.1). К ним относятся изменения, связанные с научно-техническим прогрессом, неопределенности разной природы, случайные помехи и др. Отсутствие контроля часто связано с недостатком знаний и поэтому может быть временным. При исследовании операций неконтролируемые факторы классифицируют как фиксированные, случайные и неопределенные [5].

Фиксированные неконтролируемые факторы — это факторы, значения которых можно определить, используя объективные закономерности. Устойчивые причинно-следственные связи и закономерности объективно существуют в биоценозе, социуме, химии, лингвистике, психологии, экономике. Манипулятор часто пользуется тем, что люди не знают о существовании тех или иных законов.

К случайным неконтролируемым факторам относится температура воздуха, скорость ветра, время безаварийной работы деталей и узлов, сезонные изменения цен на товары и услуги и др. Подобные процессы, протекающие во времени, называют случайными. Случайные факторы — это проявления случайных процессов, оказывающих влияние на ход информационной операции. Если существует взаимно однозначное соответствие между значением случайного фактора и вероятностью его наступления, то говорят, что задан закон распределения случайного процесса. Знание этого закона позволяет определить вероятность наступления нежелательного события и оценивать риски.

Неопределенным называют фактор, для которого известна только область допустимых его значений. Для него неизвестны законы изменения и вероятности распределения. Неопределенные факторы принято делить на три класса. Во-первых, это факторы, связанные с нечеткостью определения цели. Во-вторых, это факторы, связанные с недостаточной изученностью каких-либо процессов и явлений (природные факторы). В-третьих, это факторы, связанные с действиями заинтересованных лиц, в том числе конкурентов.

Для природных факторов определена область их возможных значений, т. е. границы, в пределах которых они могут меняться (например, максимальное и минимальное значения). Изучение природных факторов, процессов и явлений является предметом естественных наук — от наблюдений и описаний до установления закономерностей. В результате открытия новых законов, неопределенные природные факторы «переносят» в класс случайных, а затем в класс детерминированных факторов.

Действия заинтересованных лиц направлены на овладение капиталом и властью [4]. К этим целям одновременно стремятся множество бизнесменов и политиков. Стремление к овладению капиталом и властью выражается в контроле рынка, победе на выборах, соревнованиях, конкурсах и т.п. Эти люди, компании и партии образуют множество конкурентов. Кроме них существует множество заинтересованных лиц, преследующих свои цели, но не участвующих в конкурентной борьбе [4]. Однако их деятельность отражается на итогах информационной операции.

3. Этапы ситуационного анализа

Ситуационный анализ является фундаментом обоснования информационной операции, основой ее разработки, планирования и реализации. К его началу нужно знать формулировку цели (проверенную на подверженность манипуляции [1]), а также минимизировать неопределенности, нечеткости представлений о задачах и неполноте исходных данных. Цель операции определяет предметную область и содержание собираемой информации. Рассмотрим основные этапы ситуационного анализа.

Этап 1. Моделирование проблемной ситуации. Следует начинать с детального её описания, а затем пытаться создать качественную и количественную модель ситуации. Разработка количественной модели часто сталкивается с принципиальными трудностями. Если объект сложен, а моделирование дорого, деньги могут быть потрачены, а результат не получен. Поэтому разрабатывать количественную модель не всегда обязательно.

Этап 2. Формирование перечня источников информации. Эксперты, зная цель операции и направления ситуационного анализа, а также данные моделирования, формируют перечень источников информации. Последние классифицируют на первичные, полученные исследователем от объектов воздействия; вторичные, информация от которых была собрана для других целей; открытые и закрытые (конфиденциальные); бесплатные и платные; публикуемые и непубликуемые; электронные, печатные, медийные и др. Эти источники информации используются для создания баз исходных данных и знаний. База знаний — это совокупность детерминированных и случайных факторов, влияющих на

ход информационной операции. База данных включает информацию о контролируемых и природных факторах, а также неопределенных факторах, связанных с действиями конкурентов и других заинтересованных лиц. По мере изменения обстановки в процессе операции проводится дополнительный анализ ситуации. С его помощью базы данных и знаний поддерживаются в актуальном состоянии.

Этап 3. Ранжирование источников информации по степени важности методом экспертных оценок [1].

Этап 4. Формирование экспертами бюджета работ, связанных с ситуационным анализом. Если он ограничен, то они разрабатывают предложения, с какими источниками информации работать, а от каких отказаться.

Этап 5. Разработка плана проведения ситуационного анализа.

Этап 6. Оформление и заключение договоров, приобретение информации.

Этап 7. Формирование и поддержка в актуальном состоянии базы исходных данных и знаний.

4. Выявление опасностей

В информационных операциях события часто являются результатом информационных воздействий. Нередко они приводят к негативным последствиям — опасностям. Выявление опасностей связано с описанием их источников, а также путей (сценариев) их реализации. Оно имеет фундаментальное значение при планировании и проведении информационных операций. Своевременное выявление опасностей позволяет избежать или свести к минимуму ущерб от них. Поэтому после проведения ситуационного анализа нужно выявить опасности, связанные с нежелательными событиями – инцидентами. Инцидент — это событие, прерывающее устоявшийся процесс. Например, дорожные инциденты — поломка автомобиля или авария — нарушают процесс дорожного движения.

Предварительное выявление опасностей включает следующие этапы:

• определение перечня возможных событий и их взаимосвязей;

• определение показателей опасности событий;

• ранжирование событий по степени опасности и определение перечня возможных инцидентов;

• анализ возможных причин эволюции ситуации от исходного события до инцидента;

• анализ возможных путей эволюции ситуации после инцидента;

• описание сценариев информационной операции на основе наиболее опасных инцидентов.

Результатом этих исследований является: описание возможных инцидентов; источников и факторов опасности, условий возникновения и развития инцидентов; предварительная оценка опасности. При значительной опасности или недостаточности предварительных оценок, можно провести детальный анализ и оценку опасности, выработать рекомендации по ее уменьшению и т.д. Для выявления опасностей используют сравнительный метод, причинно-следственный анализ, анализ сетей событий, логические диаграммы и др. [1].

Сравнительный метод выявления опасностей основан на анализе архивных материалов. Суть его в следующем. Из архивов организации (корпорации, партии) извлекают материалы, связанные с подобными ситуациями. Аналогичные материалы ищут в Интернете, электронных базах данных, в библиотеках. После сбора информации проводится сравнительный анализ последствий былых событий. Вводятся поправки на изменение условий и обстановки за прошедшее время, в частности, на изменения в законодательстве, политической и экономической конъюнктуре, внешних воздействиях. Выявляются возможные источники угроз, оценивается вероятность и величина ущерба.

Причинно-следственный анализ широко применяется на всех этапах информационной операции, начиная с разработки ее концепции. Часто он основан на «мозговом штурме» [6]. Руководитель информационной операции предлагает опытным специалистам, знакомым с анализируемыми процессами, задавать вопросы и ставить проблемы, связанные с этапами её проведения. На первом шаге ставятся общие вопросы, возникающие при организации и ведении информационной операции. Затем проводится классификация вопросов по типам и этапам операции. При анализе каждой стадии операции ставятся новые вопросы. Ищутся ответы на вопросы о причинах, последствиях и мерах безопасности. Затем вырабатываются приемлемые действия. Основой анализа является новая информация об условиях информационной операции, изменениях в законодательной и финансовой сфере, политической конъюнктуре и т. п. Аналитическая группа должна включать специалистов по всем аспектам информационной операции — юристов, маркетологов, политтехнологов и др. Очень важна высокая компетентность членов группы [6]. Причинно-следственный анализ особенно полезен на начальной стадии операции, когда еще нет информации для использования более точных методов – таких, как анализ сети событий.

5. Анализ сетей событий

Для выявления опасностей широко используется анализ сетей событий (АСС). В его основе лежат методы математической логики, сетевого планирования и управления, теории графов и случайных процессов. Рассмотрим основные определения, используемые в АСС [1].

Инцидент — нежелательное отклонение состояния системы (социальной, экономической, финансовой или иной) от нормы или ожидаемого результата. *Сеть событий* — граф, вершинами которого являются события, а ребра характеризуют причинно-следственные связи между ними. Сеть событий — это графическая логическая модель, дающая систематическое описание временной последовательности событий. Выход — конечное событие, являющееся результатом исходного. Каждое событие, следующее за исходным, условно по отношению к предшествующему. *Условие (логические ворота)* — логическая связь между событиями. Условие «*и*» объединяет одновременно происходящие события. Условие «*или*» означает, что для события достаточно одного из предыдущих.

Анализ сети событий основан на поиске и изучении множества его путей. *Путь* — это последовательность событий, приводящих к выходу. Вероятность последнего можно рассчитать, зная вероятности предшествующих событий. Поэтому АСС широко применяется при оценке рисков. Каждый путь соответствует одному выходу сети событий. Можно выделить два типа АСС.

Послеинцидентный АСС используется для оценки результатов произошедшего инцидента и разработки мероприятий по его недопущению в будущем. Популярное название послеинцидентного АСС — «разбор полетов». При этом инцидент играет роль исходного события. Одна из целей построения сети событий — определить возможные его последствия (выходы). Строится временная последовательность спровоцированных инцидентом событий.

Доинцидентный АСС направлен на предотвращение возможного инцидента. Он изучает события, способствующие и мешающие возникновению инцидента. При этом инцидент играет роль нежелательного конечного события — выхода. Наряду с ним рассматриваются и желательные выходы. Доинцидентный анализ важен для выявления возможных причин инцидента.

Опишем этапы программы анализа сети событий.

Этап 1. *Определение исходного события* дает начало построению сети событий. Для этого оценивается корреляция событий и опасных последствий. Используются статистические данные об имевших место инцидентах.

Этап 2. *Определение функции безопасности и фактора развития риска.*

Функция безопасности прерывает последовательность от исходного события до опасного выхода. Наиболее часто она используется в доинцидентном анализе. Фактор развития риска — это фактор, который может изменить выход. Наиболее часто он используется в послеинцидентном анализе.

Этап 3. *Построение сети событий.*

Сеть событий графически иллюстрирует их хронологическую последовательность. Поэтому ее строят слева направо, начиная с исходного события (рис.2). Па сети событий показывают только вершины, влияющие на выход. События отмечают кружками, в которых указывают их наименования (заголовки) и обозначения. Из каждой вершины выходят стрелки (дуги), соответствующие вариантам развития событий. Последовательность дуг и вершин образует путь. Каждый путь характеризуют комбинацией обозначений. Пути могут иметь разное количество вершин. Например, на рис. 2 имеется 3 пути — $C_0A_1A_2$, $C_0Б_1Б_2$, $C_0B_1B_2Б_2$ с 3-4 вершинами.

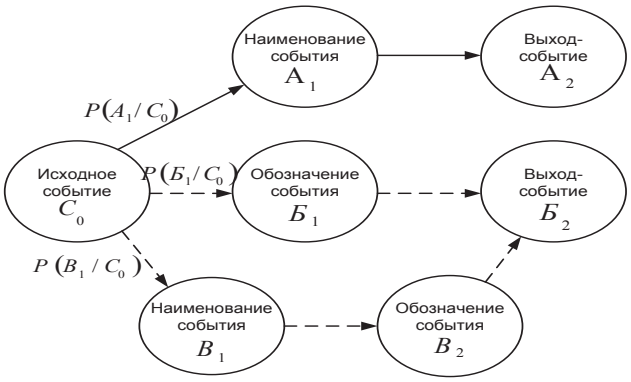

Рис. 2. Сеть событий

Этап 4. *Классификация выходов.*

В послеинцидентном анализе исходное событие — инцидент. В доинцидентном анализе ищут желательный выход, соответствующий отсутствию инцидента. По его результатам составляется список условий инцидентов и мер по восстановлению безопасности.

Выходами сети событий могут быть как желательные события, так и инциденты. Если цель АСС — оценка риска инцидентов, то достаточно проанализировать только относящиеся к ним выходы. Выходы можно классифицировать также в зависимости от величины полезностей (ущербов). Например, выход приемлем (или неприемлем), если его полезность находится на высоком (или низком) уровне. Пути, ведущие к неприемлемым выходам, надо исключать.

Этап 5. *Оценки условных вероятностей.*

Для каждой дуги, выходящей из кружка с заголов-

ком события (рис.2), указывают ее вероятность при условии, что данное событие произошло (т. е. условную вероятность). Таким образом, сумма условных вероятностей всех дуг, выходящих из любого кружка с заголовком события, должна быть равна 1,0. Например, на рис. 2 для каждой дуги, выходящей из кружка, соответствующего исходному событию, указана ее вероятность, при условии, что имело место исходное событие. Сумма указанных условных вероятностей равна 1

$$P(A_1/C_0)+P(Б_1/C_0)+P(B_1/C_0)=1.$$

Источниками информации об условных вероятностях могут быть мнения экспертов, статистика, записи об имевших место событиях и т. п.

Этап 6. *Оценка вероятностей событий-выходов.*

Условная вероятность события — это вероятность того, что событие произойдет, если произошли другие события. Пусть $P(A)$ — вероятность события A; $P(B/A)$ — вероятность последующего события B, при условии события A; $P(AB)$ — вероятность событий A и B. По определению условной вероятности

$$P(B/A)= P(AB)/P(A). \qquad (9)$$

Если известна вероятность предшествующего события A и условная вероятность $P(B/A)$, то, согласно (9), вероятность событий A и B равна

$$P(AB) = P(B/A)\cdot P(A). \qquad (10)$$

Зная вероятность исходного события и условные вероятности событий, можно оценить вероятности путей и событий-выходов. Последовательно применяя формулу (10), получаем, что вероятность пути равна произведению вероятности исходного события и условных вероятностей всех последующих его событий. Например, вероятность пути $C_0A_1A_2$, отмеченного на рис.2 сплошными дугами, равна произведению вероятности исходного события P_0 и условных вероятностей последующих событий A_1 и A_2

$$P(C_0A_1A_2) = P(A_2/A_1)\cdot P(A_1/C_0)\cdot P_0.$$

Заметим, что на рис. 2 к выходу A_2 ведет только один путь $C_0A_1A_2$. Поэтому вероятность $P(A_2)$ выхода A_2 равна вероятности этого пути

$$P(A_2) = P(C_0A_1A_2) = P(A_2/A_1)\cdot P(A_1/C_0)\cdot P_0.$$

Предположим теперь, что к выходу ведет несколько путей. Вероятность такого выхода равна сумме произведений вероятности исходного события и условных вероятностей событий для всех путей, ведущих к этому выходу. Например, к выходу $Б_2$ на рис. 2 ведут пути $C_0Б_1Б_2$ и $C_0B_1B_2Б_2$. Вероятность $P(C_0Б_1Б_2)$ пути $C_0Б_1Б_2$, отмеченного на рис. 2 прерывистыми дугами, равна произведению вероятности исходного события P_0 и условных вероятностей последующих событий $Б_1$ и $Б_2$

$$P(C_0Б_1Б_2)= P(Б_2/Б_1)\cdot P(Б_1/C_0)\cdot P_0.$$

Вероятность $P(C_0B_1B_2Б_2)$ пути $C_0B_1B_2Б_2$, отмеченного на рис. 2 штрих-пунктирными дугами, равна произведению вероятности исходного события P_0 и условных вероятностей последующих событий $B_1,B_2,Б_2$

$$P(C_0B_1B_2Б_2)= P(Б_2/B_2)\cdot P(B_2/B_1)\cdot P(B_1/C_0)\cdot P_0.$$

Тогда вероятность $P(Б_2)$ выхода $Б_2$ равна сумме вероятностей обоих путей, ведущих к этому выходу

$$P(Б_2) = P(C_0Б_1Б_2)+P(C_0B_1B_2Б_2)=$$
$$=P(Б_2/Б_1)\cdot P(Б_1/C_0)\cdot P_0+ P(Б_2/B_2)\cdot P(B_2/B_1)\cdot P(B_1/C_0)\cdot P_0.$$

Этап 7. *Проверка выходов* обычно проводится независимыми экспертами.

6. Прогноз последствий и оценка вероятности

Анализ сети событий дает «портрет» выходных событий в системном, логическом и документированном виде. Сети событий — это графическое представление логических моделей или таблиц истинности [7]. Доинцидентный АСС указывает сильные и слабые стороны систем безопасности (предупреждения инцидентов). Послеинцидентный АСС определяет множество возможных выходов из данного инцидента.

Оценка вероятности события основана на использовании статистических данных, математическом и имитационном моделировании, анализе сети событий, внешних причин и человеческого фактора. Оценка вероятности события может основываться на статистических данных, например, о частоте подобных событий в прошлом (их числе за определенный период времени). Однако такая оценка часто затруднена из-за отсутствия нужных объемов статистических данных. Оценку вероятности события можно получить путем математического и имитационного моделирования. Точные оценки могут дать имитационные модели, содержащие множество параметров и переменных. Однако они малопригодны для исследования общих закономерностей явлений большой размерности. Альтернативу имитационным моделям представляют адаптивные архетипы [1,2-4,6,8,9]. Они содержат минимальное количество параметров и не претендуют на детальное описание явлений, но дают качественную картину поведения системы в целом, помогают понять основные механизмы рассматриваемых процессов. Промежуточное по сложности положение занимают математические модели оценки вероятности события, содержащие наиболее существенные параметры моделируемых процессов.

Экспертно-математические модели оценки вероятности событий на основе АСС. Принципы оценки вероятности событий-выходов, на основе известных

вероятностей исходных и промежуточных ее событий, были рассмотрены выше (этап 6 АСС). АСС позволяет получать оценку вероятности инцидента, являющегося следствием предшествующих событий в сети. Для этого используется *сетевой метод*. Суть его заключается в том, что эксперты последовательно оценивают вероятности наступления событий, начиная с исходного. Если эксперты уже оценили вероятность предшествующего события A и условную вероятность $P(B/A)$, то, согласно (9), вероятность событий A и B равна (10). Такой подход позволяет экспертам оценивать вероятности наступления последующих событий.

В общем случае сетевой метод предполагает создание группы экспертов, которая оценивает вероятности связанных событий. Предположим, например, что функциональная связь событий в сети такова

$$S_k=f(S_1,S_2,...,S_{k-1}),$$

где S_1 и S_k — исходное и конечное события; $S_2,...,S_{k-1}$ — промежуточные события; f — логическая функция своих переменных. В простейшем случае f включает только операции «и» (конъюнкции). Тогда событие S_k является следствием всех предыдущих событий $S_1,S_2,...,S_{k-1}$. Если эксперты оценили вероятность исходного события S_1 и условную вероятность события S_2, то вероятность наступления последнего вычисляется по формуле (10), где $A=S_1$, $B=S_2$. Если эксперты смогли оценить условные вероятности событий $S_3,...,S_{k-1},S_k$, то последовательно оцениваются вероятности их наступления по формуле (10). На их основе можно оценивать вероятности путей — последовательностей событий от исходного до конечного. Разумеется, функция f может иметь и более сложную структуру. Например, вместо операции «и» может осуществляться операция «или».

Процедура расчленения событий. Предположим, что эксперты не могут оценить вероятность некоторого события S_i. В этом случае проводят процедуру его расчленения. Она состоит в следующем: для события S_i указывают совокупность событий $\left(S_{ij}, j=\overline{1,n_i}\right)$ общим числом n_i, от которых зависит событие S_i. Затем вводят событие $S_{i-1}=f(S_{i1},S_{i2},...,S_{in})$, состоящее в совокупности событий $\left(S_{ij}, j=\overline{1,n_i}\right)$. После этого оценивают условную вероятность $Q(S_i/S_{i-1})$ события S_i, если произошло событие S_{i-1}. Затем эксперты оценивают вероятности P_{ij} событий $\left(S_{ij}, j=\overline{1,n_i}\right)$ и подсчитывают вероятность P_{i-1} события $S_{i-1}: P_{i-1}=P(P_{i1},P_{i2},...,P_{in})$. Тогда вероятность события S_i равна $P_i=Q_i(S_i/S_{i-1})P_{i-1}$. Если эксперты не в состоянии оценить вероятность P_{ij} того или иного события S_{ij}, то применяется процедура его расчленения и т. д. В конце концов, описанный выше процесс приведет к достаточно простым событиям, вероятности наступления которых уже могут быть определены экспертами.

Для оценки вероятности событий-выходов на основе вероятности предшествующих событий может быть полезно и имитационное моделирование. Однако оно часто затруднено большой размерностью задачи (множеством компонент и параметров данных), неустойчивостью социально-экономических систем, неформальными компонентами (такими, как социальная активность и психология, человеческий фактор [3]).

Вероятность последовательности тех или иных событий зависит от объективных и субъективных причин. Объективные причины относятся к неконтролируемым факторам и управлять ими невозможно. Их нужно выявлять и учитывать при планировании и проведении информационных операций. Субъективные причины зависят от субъекта информационной операции — личности, партии, корпорации. Их можно контролировать, а значит — ими можно управлять. Влияние человеческого фактора на вероятность события анализируют в двух направлениях. Во-первых, человек рассматривается как оператор, который может ошибиться. Оценка вероятности его ошибки относится к компетенции инженеров-психологов. Определяются также последствия такой ошибки. Второе направление изучает возможное событие и его последствия, как функцию деловых и моральных качеств человека. Для раскрытия потенциала личности в информационной операции используют прогрессивные и интеллектуальные механизмы [8,9].

Оценка вероятности события может быть основана на анализе *внешних факторов*. Для этого используются описанные выше приемы АСС. Во-первых, инциденты могут происходить под влиянием внешних факторов, являющихся результатом целенаправленных внешних воздействий. При этом их вероятность прямо зависит от ожидаемых выигрышей внешних игроков, ставок в большой игре. Если это доступ к финансовым, сырьевым или административным ресурсам, то вероятность инцидентов повышается. И тогда внезапно происходящие события, маловероятные в обычной обстановке, приводят к масштабному ущербу.

Во-вторых, внешние факторы могут носить случайный характер. Пример — скачки цен на нефть вследствие серии террористических актов. Анализ внешних факторов в экономике, как известно, базируется на ис-

следовании конъюнктуры и состояния мировых рынков, политической обстановки в стране и мире, статистическом и имитационном прогнозировании. Оценки вероятности внешних факторов полезны для построения сценариев развития событий. Предварительный анализ внешних событий не гарантирует от неприятностей, если последствия воздействий окажутся тяжелыми, а вероятности их наступления большими. Основываясь на результатах этих оценок, можно определить, нужен ли более детальный анализ внешних событий, и принимать меры по снижению риска.

Информационное воздействие может инициировать или предупредить нежелательное событие (инцидент). Например, оно может спровоцировать ажиотажное изъятие вкладов клиентами банков или успокоить их. В свою очередь, нежелательное событие приводит к негативным последствиям — ущербам (экономическим, экологическим, социально-политическим и др., см. рис. 3).

Риск, понимаемый как ожидаемая величина потерь, равен произведению вероятности события и величины ущерба от него. Оценка риска основана на определении опасностей, построении и анализе сетей событий, оценке вероятности событий и ущербов от них. Специфика ущерба определяет название риска: экономический, социально-политический, финансовый, коммерческий и др. Все эти риски можно пересчитать в экономические, если известны операторы Q_i пересчета i-го риска в экономический риск, $i = \overline{1,n}$.

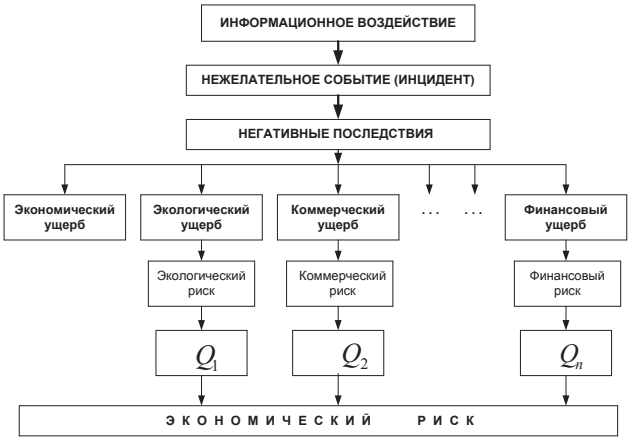

Рис. 3. Оценка рисков информационных воздействий

Литература

1. Бухарин С.Н., Цыганов В.В. Методы и технологии информационных войн. - М.: Академический проект. 2007.-387с.

2. Цыганов В.В., Бухарин С.И. Информационные войны в бизнесе и политике. Теория и методология. - М.: Академический проект, 2007. – 324с.

3. Цыганов В.В. Адаптивные механизмы и высокие гуманитарные технологии. Теория гуманитарных систем. – М.: Академический проект, 2012. - 351с.

4. Цыганов В.В., Бородин В.А., Шишкин Г.Б. Интеллектуальное предприятие. Механизмы овладения капиталом и властью. М.; Университетская книга, 2004.

5. Гермейер Ю.Б. Введение в теорию исследования операций. М.: Наука, 1971.- 398с.

6. Шульц В.Л., Цыганов В.В. Модернизация системы национальной безопасности. – М.: Наука, 2010.- 216с.

7. Хенли Э., Кумамото Х. Надежность технических систем и оценка риска. М.: Машиностроение, 1984.

8. Цыганов В.В., Бочкарева Ю.Г. Прогрессивные механизмы информационного воздействия в социально-экономических системах // Информационные войны, №1, 2012.С. 2 – 8.

9. Цыганов В.В., Бочкарева Ю.Г. Интеллектуальные механизмы информационного воздействия // Современные проблемы науки и образования, №4, 2012. URL: http://www.science-education.ru/104-6760.

Материал поступил в редакцию 12. 01. 2014 г.