СЦЕНАРНОЕ МОДЕЛИРОВАНИЕ В УПРАВЛЕНИИ БЕЗОПАСНОСТЬЮ СЛОЖНЫХ ОРГАНИЗАЦИОННЫХ СИСТЕМ

Чернов И.В.
Институт проблем управления им. В.А. Трапезникова РАН, Москва, Россия
chernov@ipu.ru

Аннотация. Рассмотрены проблемы повышения эффективности управления обеспечением национальной безопасности России в информационной сфере. Выделены базовые уровни обеспечения безопасности и проведен анализ основных направлений развития методологии сценарного анализа и моделирования как инструмента поддержки принятия решений. Изложены результаты разработки средств автоматизации сценарных исследований.

Ключевые слова: сценарий, сценарное моделирование, событие, модель, безопасность, неопределенность, противодействие, программно-аналитический комплекс.

Введение

Сложившаяся политическая ситуация, а также беспрецедентно жесткое и широкомасштабное санкционное давление в отношении России привели к существенному нарастанию существующих и появлению принципиально новых и крайне опасных стратегических угроз национальной безопасности (НБ) Российской Федерации [1-3]. Реалии настоящего времени ставят перед Россией целый ряд принципиально новых неотложных как оперативных, так и нацеленных на долгосрочную перспективу задач обеспечения безопасного и устойчивого развития страны с учетом новых угроз и ограничений.

Многофакторный и многоцелевой характер данных угроз, точечный (а по ряду направлений – скрытный) и ориентированный на имеющиеся уязвимости социально-экономической системы нашей страны выбор способов и механизмов политического и экономического давления диктуют острую необходимость повышения эффективности государственного управления в сфере обеспечения НБ России [2-6].

1. Уровни безопасности сложных организационных систем

Как следует из определения, данного в Стратегии национальной безопасности [1] и в соответствии с направлением сценарного исследования, безопасность нашей страны является необходимым условием реализации такого сценария ее развития, при котором обеспечиваются национальные интересы Российской Федерации – объективно значимые потребности личности, общества и государства в безопасности и устойчивом развитии. Этот общий сценарий состоит из сценариев, которые иерархически обеспечивают реализацию стратегических национальных приоритетов страны.

Если рассматривать страну как объект управления, то в применении к информационной сфере можно выделить несколько уровней безопасности (Таблица 1)

Таблица 1. Уровни управления безопасностью сложных систем

Уровни безопасности	**Цель воздействий**	**Направления воздействия**	**Ограничения на управление**
Надструктурный, системообразующий	Навязывание правил формирования базовых связей структур (строй, законы и т.п.)	Идеология, культура, мораль. Экономика. Инфраструктура. Политическая система. Социальная система	Проблема обнаружения стратегических последствий. Противодействие: история, традиции, религия, менталитет
Структурный, стратегический	Внесение уязвимостей в структуру	Структура безопасности государства (экономическая, социальная, военная, информационная…)	Необходимость соблюдения навязываемых структурообразующих правил (демократия, рынок и т.п.)
Внутриструктурный, тактический	Активизация структурных уязвимостей. Информационные атаки	Информационные атаки, направленные на уязвимые места. Формирование и активация угроз	Ограничено структурой со всеми ее уязвимостями. Борьба не

Уровни безопасности	Цель воздействий	Направления воздействия	Ограничения на управление
			с причинами, а со следствиями

Неэффективное управление на этих уровнях ведет к внесению в объект уязвимостей, посредством использования которых осуществляются попытки внешнего воздействия и возникают угрозы, снижающие возможности суверенного управления. Повышение эффективности обеспечения НБ государства является одной из наиболее сложных проблем теории и методологии организационного управления и целого ряда смежных научных дисциплин [2]. Основная сложность заключается в том, что национальная безопасность и как предметная область, и как объект управления представляет собой мультифункциональную распределенную многопараметрическую слабоструктурированную, и, как следствие – плохо формализуемую (за исключением крайне редко встречающихся частных задач) систему, характеризующуюся [3-6]:

- существенной зависимостью от состояния и тенденций развития ситуации во внешней среде, а также связанных с ними угроз и рисков;
- территориальной распределенностью широкого множества объектов управления различного типа;
- большим числом и сложностью функциональных, материально-финансовых, информационных и т.д. взаимосвязей (взаимозависимостей) между ними;
- размытостью границ взаимовлияния и взаимодействия элементов системы;
- широким спектром функциональных задач обеспечения НБ, содержательно дифференцируемым по целому ряду в различной степени самостоятельных направлений в рамках рассматриваемой предметной области;
- крайне широким множеством разнородных качественных и количественных показателей и параметров, отражающих обеспечиваемый уровень НБ по различным направлениям;
- наличием явных или существенных противоречий в описании или оценке ситуации;
- подвижность структуры, обусловленную высокой степенью вариативности элементов и их взаимосвязей;
- высоким уровнем неопределенности и «информационной размытости»;
- большим количеством различных исследуемых аспектов и связанных с ними показателей и параметров, а также не всегда очевидных связей между ними;
- потребностью существенных затрат ресурсов и времени для решения функциональных задач управления обеспечением национальной безопасности;
- слабой структурированностью или ее отсутствием;
- принципиальной сложностью построения точных математических моделей проблемной ситуации с использованием классических моделей и методов.

В значительной степени преодоление трудностей управления подобными объектами обеспечивается применением методологии сценарного анализа, базирующейся на процессах разработки и исследования имитационных моделей, создаваемых на основе аппарата знаковых и функциональных графов [2-6] и позволяющей формировать целевой прогноз поведения как самого объекта управления, так и его окружения (внешней среды). Предлагаемый подход в процессе исследования масштабных, крайне важных и одновременно с этим слабоформализуемых (не поддающихся строгой формализации) проблем позволяет оперировать широким множеством различных по своей природе количественных и качественных показателей (в том числе не всегда прямо сопоставимых), а также учитывать характер причинно-следственных связей между ними.

2. Понятийный аппарат сценарного исследования

Введем несколько определений, необходимых для формирования общей схемы методологии сценарного исследования.

Системный элемент – формальное описание рассматриваемого подмножества системы, которая в рамках данного исследования представляет собой заданный набор объектов, объединенных общими отношениями (взаимодействиями) и обладающих определенными свойствами, например, выполняющие определенные функции и задачи.

Экспертно-значимая декомпозиция исследуемой системы на системные элементы – объединение данных элементов по заданному набору системных параметров. Естественная группировка системных

элементов по традиционным стратам: экономическая, информационная, политическая, военная и др. страты.

Расширенное фазовое пространство включает объединение (прямое произведение) фазового пространства исследуемой системы и внешнего пространства. В качестве элементов фазового пространства могут выступать аналитические данные моделирования, например, типы динамик поведения факторов.

Разбиение расширенного фазового пространства – подмножество данного пространства, переменные которого выделяют по определенному критерию (например, определенные социальные группы, экономические методы воздействия, информационные операции и др.). Разбиения фазового пространства позволяют формировать качественно различные сценарии изменения обстановки. В сценарном исследовании набор таких критериев (правила выбора) и их значимость для реализации целей управления можно задавать экспертным путем (в этом случае говорят об экспертно-значимых разбиениях).

Правила выбора экспертно-значимых разбиений – критерий, по которому происходит выделение экспертно-значимых разбиений.

Состояние объекта управления – совокупность значений эндогенных и экзогенных переменных (точка в расширенном фазовом пространстве) объекта управления (ОУ).

Модель измерения состояния ОУ – совокупность правил фиксации (определения) состояний ОУ.

Событие – фиксация текущего состояния ОУ посредством модели измерения состояний (точка в расширенном фазовом пространстве).

Динамическая модель поведения ОУ – совокупность состояний ОУ, фиксированных на основе модели измерения в заданные моменты времени. Множество таких состояний представляет собой траекторию поведения ОУ.

Экспертно-значимое событие (ЭЗС) – выделенное в соответствии с правилами выбора состояние исследуемой системы: точка в экспертно-значимом разбиении фазового пространства.

Шкала траекторий – шкала модельного времени (множество моментов времени) определяет моменты фиксации траектории поведения объекта в соответствии с правилами выбора.

Шкала событий – дискретная шкала, определяющая последовательность ЭЗС.

Квазиинформационная гипотеза (КИГ) – формальное описание неопределенности в определённый момент времени, учитываемой при формировании сценариев. В КИГ входит возможная реакция ОУ, изменение структуры, изменение свойств отношений взаимодействия и т.п.

3. Общая схема формирования сценария

Используя термины понятийного аппарата сценарного исследования, разработана общая схема сценарного исследования (рис. 1), которая легла в основу программно-аналитического комплекса сценарного моделирования, разработанного в лаборатории Сценарного управления Института проблем управления РАН.

Основная задача при генерации сценариев изменения обстановки – описать экспертные неформализованные знания о предметной области исследования формальными математическими конструкциями. Цель – создать спектр сценариев поведения системы как модели развития обстановки при различных условиях и управленческих воздействиях.

Предлагаемая схема описывает разветвленный многоуровневый механизм формирования сценария. С одной стороны, он отражает основные этапы процесса моделирования изменения обстановки при функционировании сложной системы. С другой, – при развернутом сценарном исследовании условий функционирования ОУ позволяет осуществлять различные стадии сценарных анализа и синтеза.

Результатом применения предложенной схемы является сгенерированный в автоматизированном режиме спектр сценариев (модель развития обстановки). С этой целью в схеме формирования сценария на начальном этапе формализуются три основные компоненты проблемной ситуации.

1. Основные формальные модели, описывающие совместное поведение ОУ и его окружения (системные метаэлементы, метасистема) и базирующиеся на экспертном описании проблемной ситуации (паспорт проблемы).
2. Формальная модель неопределенности – квазиинформационная гипотеза (КИГ).
3. Формализованное описание предметной области на основе выделения экспертно-значимых декомпозиций, экспертно-значимых разбиений (ЭЗР) расширенного фазового пространства и экспертно-значимых событий (ЭЗС) [5].

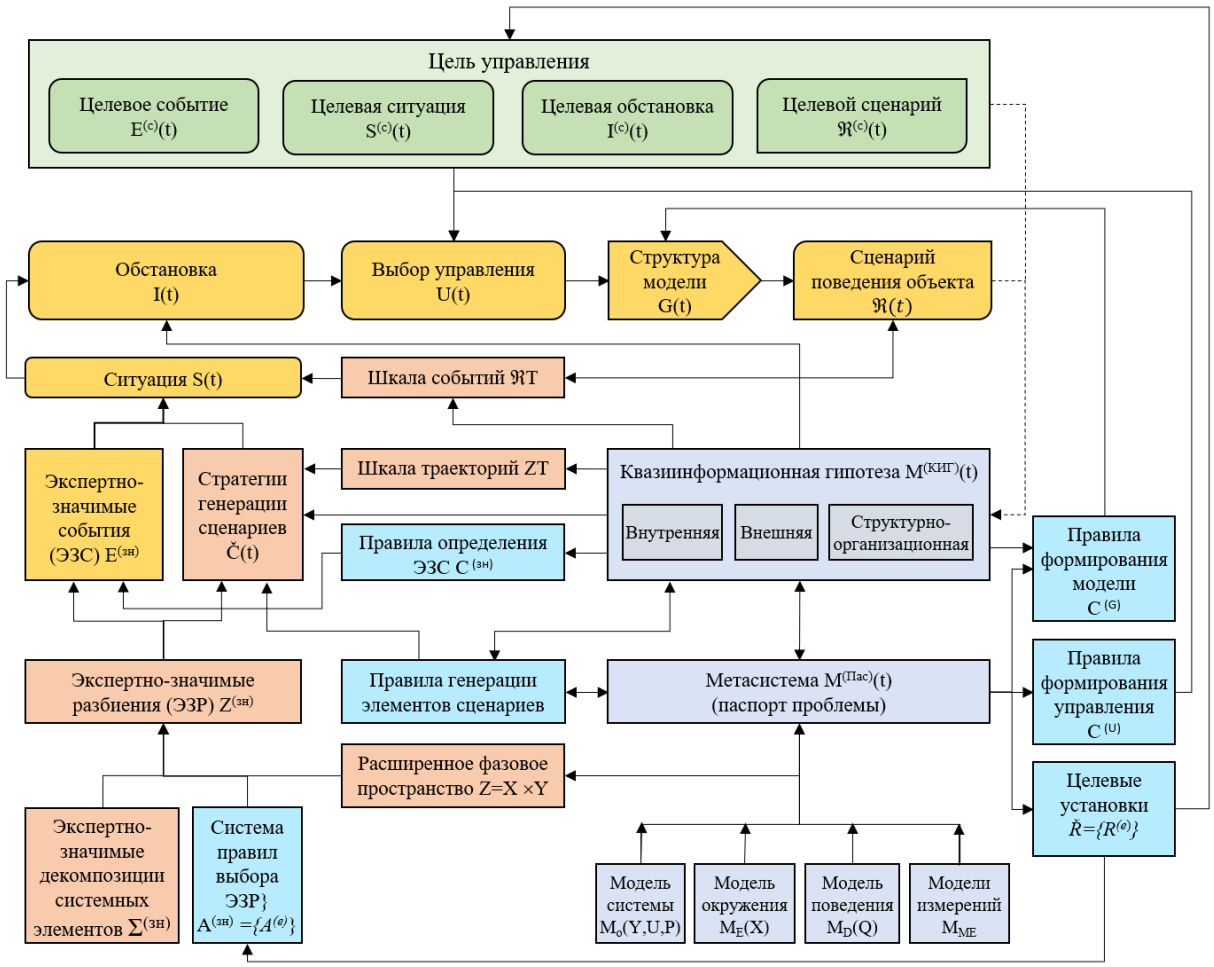

Рис. 1. Общая схема сценарного исследования

В основе сценарного исследования в широком смысле и сценарного моделирования – в узком лежит анализ данных как об исследуемом объекте (системе), так и об обстановке, влияющей на его характеристики, функционирование и развитие.

Среди параметров системы можно выделить: вектор экзогенных переменных $\boldsymbol{x} \in X$; вектор эндогенных переменных $y \in Y$; вектор управляемых переменных $u \in U$, вектор ресурсов $p \in P$ и ограничения Q, которые накладываются на поведение объекта или развитие ситуации [5].

Для сбора и представления исходных данных используется ряд системных элементов сценарной системы, представляющих собой следующие модели [5-7]:

- идентифицированная модель системы – $M_{\boldsymbol{O}}(Y;U;P)$;
- модель окружения – $M_{\boldsymbol{E}}(X)$;
- модель поведения – $M_{\boldsymbol{D}}(Q)$;
- модель измерения состояний системы – $M_{\boldsymbol{MO}}$;
- модель измерения состояния окружения – $M_{\boldsymbol{ME}}$.

Совокупность выделенных моделей является метанабором сценарной системы и служит основой создания и поддержания в актуальном состоянии паспорта проблемной ситуации:

$$\boldsymbol{M} = (M_{\boldsymbol{O}}(Y;U;P); M_{\boldsymbol{E}}(X); M_{\boldsymbol{D}}(Q), M_{\boldsymbol{MEO}}).$$

Прежде всего необходимо идентифицировать исследуемую систему как объект управления, выделив и описав параметры и связи между ними в модели $M_{\boldsymbol{O}}(Y;U;P)$. Аналогичные процедуры выполняются для экзогенных переменных в модели $M_{\boldsymbol{E}}(X)$, которые служат основой для получения спектра альтернативных сценариев, поскольку именно с ее помощью проводится анализ параметров окружения и формируются альтернативные гипотезы об изменчивости (в том числе с учетом неопределенности) внешней среды.

При формировании, а затем и исследовании сценарной модели развития ситуации в сфере безопасности сочетание обеих моделей $M_{\boldsymbol{O}}(Y;U;P)$ и $M_{\boldsymbol{E}}(X)$ в рамках составного системного элемента сценарной системы $\tilde{S}_{\boldsymbol{OE}}^{SC}$ с набором внутренних элементов и элементов окружения (y,u,p,x). Конкретный

состав элемента сценарной системы $\tilde{S}_{\boldsymbol{OE}}^{SC}$, как и состав моделей $M_{\boldsymbol{O}}(Y;U;P)$ и $M_{\boldsymbol{E}}(X)$ определяется в соответствии с целью сценарного исследования.

Модель $M_{\boldsymbol{D}}(Q)$ задает преобразование параметров системы и характер их взаимодействия с параметрами окружения, что в итоге характеризует динамику изменения фазовых состояний.

Особое место в общей схеме формирования сценариев в части представления результатов, на основе которых принимаются управленческие решения, занимает модель измерения состояний M_{MEO}. Она включает две модели: модель измерения состояния системы M_{MO} (объекта или проблемной ситуации) и модель измерения состояния внешней среды M_{ME}.

В основе любого сценария лежит определение событий $E^{(\text{зн})}$ (ЭЗС), которые формируются на основе изменяемых фазовых состояний системы. Всякий раз определение $E^{(\text{зн})}$ должно осуществляться формализовано на основе модели измерений. От выбора последней зависит формирование взгляда на обстановку и соответственно выбор конкретного управленческого решения. Следовательно, модель измерений также может являться объектом косвенного управления, зачастую реализованного в форме информационно-психологического воздействия.

Результаты сценарного исследования с помощью специализированного программного комплекса, основанного на использовании определенного математического аппарата, по сути, являются «протосценариями», поскольку для получения сценария необходимо провести смысловое соответствие полученных расчетных результатов к терминологии конкретной предметной области. Использование модели измерения состояний $M_{\boldsymbol{MO}}$ позволяет проводить качественной анализ важнейших параметров поведения исследуемого объекта или развития ситуации, что способствует их адекватной идентификации при выработке управленческих решений. В частности, можно отметить, что различные модели измерений позволяют «толковать» события в пользу того или иного субъекта действия, что является одним из направлений информационного управления. В информационном управлении модель измерения может выступать самостоятельно, не опираясь на реальные события.

Модель измерения $M_{\boldsymbol{MO}}$ регламентирует масштаб и варианты измерения объекта, так же, как и модель измерения состояния внешней среды M_{ME} для окружения объекта. Степень детализации может зависеть от цели управления, обстановки и возможностей субъекта управления. Следовательно, имеет смысл рассматривать объединённую модель измерения $M_{MEO} = (M_{MO}, M_{ME})$.

Таким образом, в качестве входной информации для системного элемента выступают значения внешних и внутренних параметров. С помощью объединенной модели $M_{MEO} = (M_{MO}, M_{ME})$ формируется по-событийно сценарно-субъективное представление о состоянии фазового пространства. Следует отметить, что подобная субъективность построения модели измерения также может являться как сильной, так и слабой стороной в управлении сложными организационными системами.

Системные метаэлементы представляют собой совокупность моделей, описывающих совместное функционирование ОУ и его окружения, включая: модель ОУ, модель окружения, модель их совместного взаимодействия, а также применяемые инструментальные средства измерения (фиксации) событий. Объединение системных метаэлементов (метасистема) составляет паспорт проблемной ситуации, который в свою очередь является основой формирования сценарной модели. Таким образом, паспорт представляет собой базу данных накапливаемой и изменяемой информации о существующих и новых ситуациях.

4. Схемы сценарного моделирования процессов управления безопасностью сложных систем

Прежде чем формировать схемы проведения сценарного моделирования необходимо провести классификацию используемых в них моделей предметной области.

Действительная модель защищаемой системы (Actual Model – AM) представляет собой модель сложной системы, максимально соответствующая реальной.

Внутренняя модель защиты системы (Internal Defense Model – IDM) используется для моделирования воздействия на объект управления (страна, регион, население и т.п.) с целью его защиты.

Внешняя модель защиты системы (External Defense Model – EDM) отображает процессы воздействия на субъект нападения.

Внутренняя модель нападения на систему (Internal Attack Model – IAM) используется для отображения воздействия на объект защиты (АЭС, население) со стороны субъекта нападения.

Внешняя модель защиты системы от дезинформации (Counterattack Malinformation Model – CMM) используется для моделирования воздействий на объект нападения с целью его дезинформации.

Внутренняя модель мониторинга системы (Internal Monitoring Model – IMD) используемая для сбора данных о реальном состоянии системы с целью выработки эффективных управленческих решений (в идеале может совпадать с действительной моделью системы AM).

Разработка методов сценарного исследования безопасности сложных систем и их уязвимости требует пояснения иерархии понятий, определяющих сущность рассматриваемых процессов: опасность, безопасность, уязвимость, угроза, ущерб, живучесть [7].

Под опасностью обычно понимают возможность возникновения обстоятельств, при которых материя, поле, энергия, информация или их сочетание могут таким образом повлиять на систему, что влечет за собой ухудшение или даже невозможность ее функционирования и развития [8]. При этом безопасность функционирования сложной системы можно определить как динамическое ее состояние, при котором могут быть предотвращены опасные состояния.

Под угрозой понимается потенциально возможное событие, действие (воздействие), процесс или явление, которые могут привести к нанесению ущерба чьим-либо интересам. Таким образом, при реализации угрозы система переходит в опасное состояние. По сути, угроза – выявленные противником уязвимости атакуемой системы и разрабатываемые им в качестве плацдарма информационного нападения (Threat - T) [7].

Ущерб – неблагоприятные для системы социальные, экономические, политические, военные и др. последствия, возникшие в результате информационного воздействия при реализации угроз (Damage – D). Выражаются в ухудшении характеристик системы (уменьшение количественного значения факторов или отрицательная динамика их поведения), либо в недостижении целей управления системой, которые были бы достигнуты при отсутствии негативных информационных воздействий.

Живучесть – способность исследуемой системы выполнять основные свои функции, несмотря на полученные повреждения (Vitality - Vit). Живучесть может определяться:

- на тактическом уровне – рассматривается только нанесенный ущерб (Vitt);
- на оперативном уровне – планируемый ущерб от реализации угроз (Vito);
- на стратегическом уровне – способность структуры системы сопротивляться возможным информационным воздействиям (Vits).

Определим информационный метаболизм системы как процесс превращения действительной модели системы в ее информационный образ, с целью поддержки процесса управление развитием, функционированием и безопасностью системы в целом. Превращение действительной системы в ее информационный образ представляет собой комплекс специальных процессов и мероприятий, обеспечивающих использование информации для повышения безопасности и удовлетворения управленческих нужд сложной системы. Чем сложнее система, тем в большей степени ее безопасность критична к частоте управленческих воздействий, следовательно, тем выше должен быть ее информационный управленческий потенциал (распределенный по времени набор инструментов и методов воздействия, а также ресурсов), а, следовательно, тем больше должна быть скорость превращения действительной (реальной) системы (AM) в ее информационный образ (IDM), что по сути является превращением материи в информацию.

Далее рассмотрим информационный аспект безопасности. С этой точки зрения уязвимостями защищаемой системы являются:

Противоречие между действительным состоянием защищаемой системы и ее информационным образом («информационная тень»), который формирует и использует система информационной безопасности ($AM \leftrightarrow IDM$).

Противоречие между действительным состоянием системы и внутренней моделью ее мониторинга, на основании которой принимаются управленческие решения. Следствием является нестабильность и неэффективность управления. Возникающие противоречия между действительным поведением (сценарием развития) AM и прогнозом ее поведения, сделанным на основе неверной модели IDM приводит к необходимости частой ее перестройки, таким образом рассматривая данную модель как функцию от времени $IDM(t)$. Проблема усугубляется тем, что реальная система также может изменяться во времени, т.е. $AM(t)$. При этом попытки модификации IDM могут привести не к структурному ее приближению к AM, а лишь к совпадению сценария для рассматриваемого этапа. Для другого этапа развития данного сценария вероятно придется в очередной раз модифицировать IDM, выполняя требование: $\mathcal{R}_i^{\mathrm{IMD}} = \mathcal{R}_i^{\mathrm{AM}}$, где $\mathcal{R}_i$ – сценарий, полученный на i-м этапе.

Противоречие между действительным состоянием защищаемой системы и ее ложным (дезинформационным) образом (EDM, «информационная тень»), который формирует система информационной безопасности для дезориентации нападающей стороны ($AM \leftrightarrow EDM$).

Противоречие между внутренней и внешней моделями обеспечения безопасности системы: отличающийся поток информации для внутреннего и внешнего потребления ($IDM \leftrightarrow EDM$).

Противоречие между действительным состоянием защищаемой системы и ее информационным образом, который формирует система информационного нападения противника для воздействия на население и органы управления (A$M \leftrightarrow IAM$).

Противоречие между внутренней моделью защиты и внутренней моделью атаки: взаимные возможности дискредитации моделей ($EDM \leftrightarrow IAM$).

Схема взаимосвязей между моделями представлена на рис. 2.

Рис. 2. Схема взаимосвязей между информационными моделями

Внутренняя информационная модель защищаемой системы представляет собой информационный образ действительности, который формируется системой информационной безопасности и предназначен для оказания направленного управляющего информационного воздействия на социум объекта управления. Таким образом, социум строит свои активные действия не в соответствии с действительностью, а руководствуясь ее управляемой «информационной тенью». В идеальном случае при отсутствии уязвимостей и/или рисков действительная модель совпадает с внутренней информационной моделью, которая при этом будет содержать только правдивую информацию. При возрастании информационных угроз и выявленных уязвимостей объекта управления внутренняя информационная модель может все больше не совпадать с действительной.

5. Схемы информационных атак

В соответствии с общей схемой сценарного моделирования, а также проведенной классификацией моделей можно выделить типовые схемы информационных воздействий (информационного управления):

- Схема «критик»: задействование выявленных противоречий между рассматриваемыми моделями со стороны информационного нападения превращается в угрозы информационной безопасности системы.
- Схема «игра на чужом поле»: информационные воздействия с целью направленного изменения внутренней модели защиты.
- Схема «игра на своих условиях»: атакующая сторона, в свою очередь, пытается навязать социуму свою информационную модель действительности, которая тем дальше от реальности, чем меньше объективный уровень информационной уязвимости системы. Кроме того, модель IAM может

оказывать влияние на исходные данные управления, заменяя систему мониторинга или внося в нее помехи.

- Схема «дальтонизм»: управление системой строится на основе целевых факторов без учета второстепенных для ЛПР (уровень уязвимости), что чревато потерей информационного потенциала.
- Схема «близорукость»: управление системой ориентировано на реализацию сиюминутных задач без учета стратегии развития (уровень реализованных угроз и последствий). Чревато переходом в глубокую защиту с консервацией или потерей будущих результатов достижения цели.

Для дезинформации системы нападения путем уменьшения воздействия на модель IAM используется внешняя модель защиты системы (EDM), которая вносит помехи в систему мониторинга атакующей стороны, а также пытается «развалить» неблагоприятный информационный образ, который может оказать негативное воздействие на социум системы. Для повышения эффективности дезинформации при формировании EDM необходимо учитывать не только реальные данные системы, но и максимальную согласованность с внутренней информационной моделью защиты (IDM).

Также, в качестве примера, можно выделить некоторые схемы противодействия информационным атакам (схемы «защиты»):

- Схема «розовые очки». Укрепление внутренней модели защиты, ликвидация признаков демонстрации противоречий между сложной системой и ее «информационной тенью».
- Схема «критик». Задействование выявленных противоречий между внутренними моделями нападения и защиты. Схема эффективна при условии успешности схемы «розовые очки».
- Схема «игра на чужом поле». Информационные воздействия с целью направленного изменения внутренней модели нападения путем ее разрушения, либо полного или частичного включения во внутреннюю модель защиты.
- Схема «ложный аэродром». Перенос противостояния в виртуальную сферу путем навязывания противнику внешней модели защиты, обеспечивающей при этом ее разрыв с действительной моделью сложной системы.
- Мониторинг со стороны противодействия информационным атакам преследует следующие цели:
- Поддержание «очевидной непротиворечивости» внутренней модели защиты системы.
- Поддержание «очевидной непротиворечивости» внешней модели защиты для дезинформации противника.
- Повышение качества принимаемых управленческих решений, основанных на данных действительной модели и внутренней модели нападения.

Мониторинг со стороны нападения преследует цели:

- Разведка и сбор данных о состоянии действительной системы.
- Обнаружение противоречий действительной системы с внешней и внутренней моделями защиты.
- Повышение качества атакующих воздействий.

6. Направления сценарного моделирования управляющих воздействий

Рассмотрим в рамках приведенной выше классификации моделей несколько подходов к сценарному моделированию управленческих воздействий как централизованных, так и групповых. Центры (субъекты) управления могут различаться по:

- сфере влияния (политика, экономика, культура, безопасность и т.д.);
- типам воздействий (изменение структуры системы, ресурсное воздействие);
- количеству рычагов, методов и ресурсов управления;
- уровню управления (федеральный, региональный, муниципальный и т.д.);
- времени существования (постоянный, временный, чрезвычайный);
- горизонту управления (стратегический, оперативный, тактический);
- целевой направленности (регулирующий, оборонительный, атакующий);
- полномочиям (устанавливающий цели, принимающий решения, консультирующий).

6.1. Централизованное управление при полной информационной прозрачности (схема 6.1)

Все центры управления имеют полную и правдивую информацию о системе: $AM = IMD = EDM$ (рис. 2). Подобная ситуация достаточно редко реализуется, поскольку полной информации о структуре систем конкурирующей стороны не имеется ни у одного субъекта управления. Такое положение соответствует схеме, представленной на рис.2.

6.2. Централизованное управление при дезинформации противника (схема 6.2)

Сторона нападения имеет доступ только к мониторинговой информации о внутренней модели обороны (рис. 3): $AM = IMD; AM \neq EDM$.

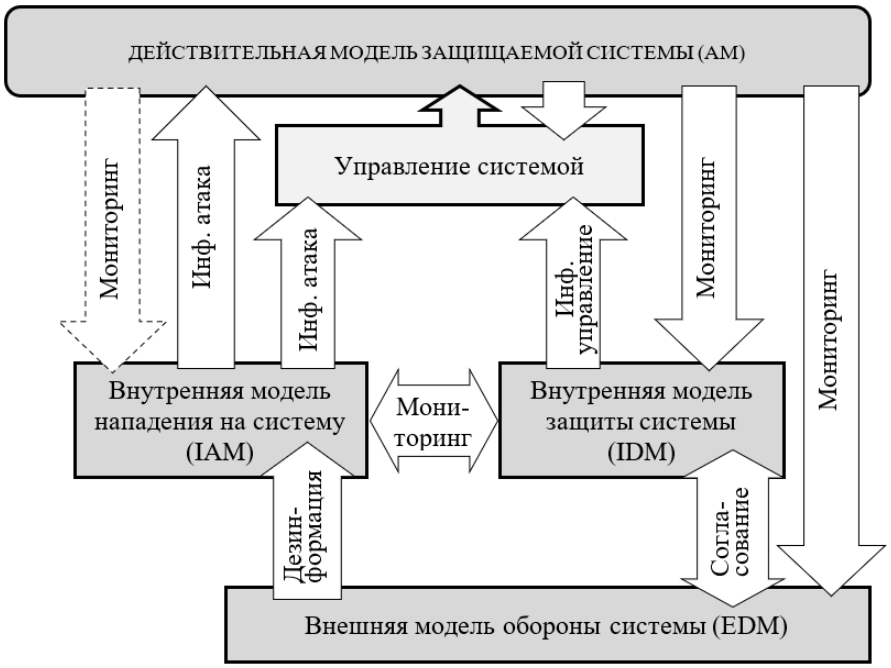

Рис. 3. Централизованное управление при дезинформации противника

Вариант сценария: сторона нападение имеет неполные данные о действительной системе, возможен «взлом» защиты, но планируемые цели могут оказаться частично или полностью нереализованными, поскольку неверно оценивается реакция атакуемой системы (стороны защиты).

6.3. Централизованное управление при ложной системе внешнего мониторинга (дезинформация системы управления) (схема 6.3)

Сторона защиты имеет доступ только к внутренней модели мониторинга системы (рис. 4). При ее аутентичности действительной модели $AM = IMD$ реализуются начальные условия описанной выше схемы 6.1. В противном случае модель мониторинга не совпадает с действительностью, или данные мониторинга хоть и верные, но запаздывают в результате действий стороны нападения.

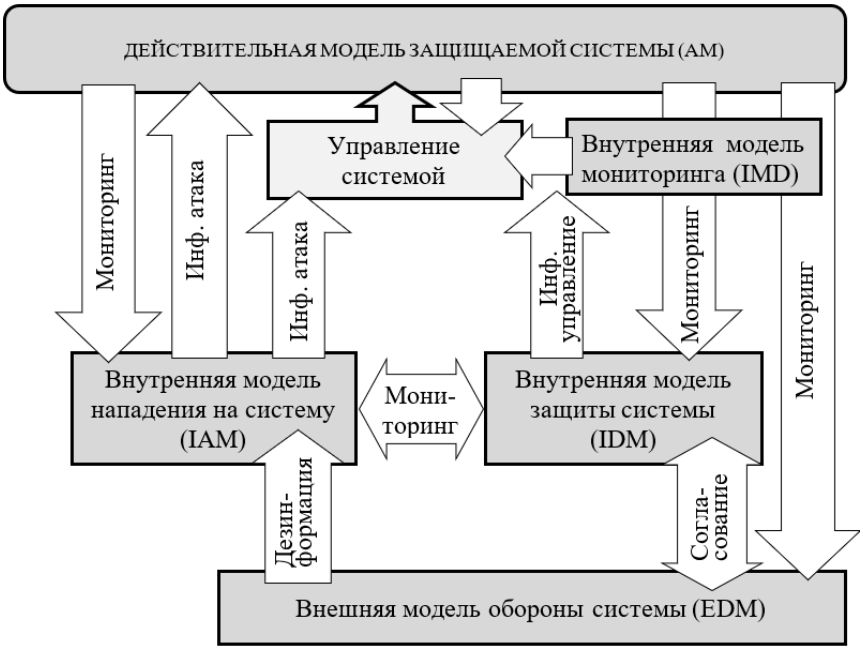

Рис. 4. Централизованное управление при ложной системе внешнего мониторинга

Вариантом рассматриваемой схемы является ситуация, когда сторона нападения оказывает воздействие на внутреннюю модель мониторинга защищаемой системы с целью ее полного или частичного поражения или взятия под контроль.

Полученные результаты в области сценарного моделирования процессов управления безопасностью сложных систем реализованы в рамках разработанного программно-аналитического комплекса, предназначенного для поддержки процессов подготовки и принятия решений в рассматриваемой предметной области [2]. Описание некоторых функций программно-аналитического комплекса в части реализации предложенных схем моделирования представлены в табл.2.

Таблица 2. Функции комплекса «Полюс» в реализации схем сценарного моделирования

Функция	**Описание и параметры функции**	**Использование функции**
Решение обратной задачи управления	Исходные данные: множество управляющих факторов, множество управляемых факторов, целевой сценарий (желаемое поведение управляемых факторов), временной промежуток оказания управляющих воздействий, временной промежуток реализации целевого сценария, временной промежуток задержки данных мониторинга. Результат: определение возможности достижение целевого сценария, программа внесения управления (импульсных воздействий) в управляющие факторы. Есть возможность решения обратной задачи на одной модели, сохранение результатов и применение результатов на другой модели.	Схема 6.1. Решение и результаты расчета обратной задачи нападения и защиты строятся и применяются на одной и той же модели. Схема 6.2. Решение обратной задачи со стороны нападения строится на ложной модели объекта управления, а результаты применяются на действительной модели. Результаты решения обратной задачи со стороны защиты строятся и применяются на одной и той же модели. Схема 6.3. Решение обратной задачи со стороны защиты строится на ложной модели объекта управления, а результаты применяются на действительной модели. Результаты решения обратной задачи со стороны нападения строятся и применяются на одной и той же модели. Схема 6.3 (вариант). Результаты решения обратной задачи применяются (вносятся управляющие воздействия) с запозданием.
Возможность создания «скрытых» структур в исходной модели	Выделение части структуры и определение ее как «скрытой» для субъекта воздействия.	Схема 6.1. Не применимо. Схема 6.2. Нападающая сторона проводит анализ и строит прогноз развития ситуации на неполных данных о структуре объекта управления. Схема 6.3. Защищающая сторона проводит анализ и строит прогноз развития ситуации на неполных данных о структуре объекта управления.
Возможность менять в ручном режиме структуру модели в процессе моделирования	На любом шаге моделирования возможны ручное или автоматическое (с использованием функциональных взаимосвязей) изменение структуры модели: активация или деактивация факторов, изменение взаимосвязей, объединение модели с другими.	Схема 6.1. Все стороны имеют полные данные о структурных изменениях. Схема 6.2. Нападающая сторона проводит анализ и строит прогноз развития ситуации на устаревших данных о структуре объекта управления. Схема 6.3. Защищающая сторона проводит анализ и строит прогноз развития ситуации на устаревших данных о структуре объекта управления.
Возможность изменения данных мониторинга, актуализирующих модель	Реализация в комплексе процедур изменения обстановки, которая заключается в получении извне данных мониторинга, которые активируют правила изменения структуры модели. Данные вводятся в ручном режиме или автоматически импортируются из	Схема 6.1. Все стороны имеют полные сведения о данных мониторинга и их влияния на структуру сценарной модели. Схема 6.2: Нападающая сторона не имеет полного или частичного представления о данных мониторинга и/или степени и направленности их влияния на перестройку структуры модели.

Функция	Описание и параметры функции	Использование функции
	сторонних программ, например, комплексов анализа информационного поля.	Схема 6.3. Защищающая сторона не имеет полного или частично представления о данных мониторинга и/или степени и направленности их влияния на перестройку структуры модели. Схема 6.2 и 6.3 (вариант). Стороны имеют ложные данные мониторинга, строя на их основе неверные представления об изменении структуры модели.

Использование программно-аналитического комплекса в качестве сценарно-прогнозной подсистемы поддержки принятия решений в сфере национальной безопасности Российской Федерации обеспечивает возможность повышения эффективности решения широкого круга прикладных задач в рассматриваемой предметной области, включающих:

- анализ корректности и достижимости сформированных целей управления;
- идентификацию «окон» уязвимости сложных организационных систем;
- диагностирование скрытых угроз реализации поставленных целей;
- выявление возможностей управления в условиях неопределенности, а также нештатных и конфликтных ситуаций;
- прогнозную оценку результативности, а также краткосрочных и долгосрочных последствий принятия решений на основе анализа синтезированных альтернативных сценариев развития обстановки при различных условиях;
- решение обратной задачи управления, заключающейся в автоматическом расчете необходимых управленческих воздействий на множество объектов управления при заданных ограничениях, обеспечивающих достижение поставленных целей управления;
- оценку характера, закономерностей и динамики развития ситуации на основе данных многофакторного мониторинга, а также выявление на их основе возможности появления неблагоприятных тенденций изменения обстановки с целью осуществления упреждающей реакции на них системы управления (соответствующей корректировки исходных целевых установок, а также состава и содержания стратегических плановых и оперативно-тактических мероприятий).

7. Заключение

Анализ современных проблем мирового развития показывает, что сегодня одним из ключевых направлений повышения эффективности управления обеспечением национальной безопасности является безусловный приоритет решения опережающих и направленные на предотвращение кризисных ситуаций задач. Таким образом, система управления безопасностью должна опираться на обоснованный целевой прогноз, формируемый на основе комплекса развитых методов и средств раннего обнаружения уязвимостей и связанных с ними угроз. Методологической основой решения задач рассматриваемого типа является сценарный прогнозный анализ альтернатив изменения обстановки как во внешней, так и во внутренней среде, а также упреждающая идентификация потенциальных угроз российскому обществу и государству.

Методология сценарного моделирования позволяет в условиях неполной информации и неопределенности использовать в качестве исходных данные как качественного, так и количественного типа и получать на выходе спектр альтернативных сценариев развития ситуации. Рассматриваемый подход в итоге позволяет не только своевременно, но и с определенным опережением оценивать возможные последствия реализации внешних угроз и наличия внутренних уязвимостей, выявлять проблемные ситуации и исследовать альтернативные направления их развития, а также осуществлять прогнозную оценку результативности принимаемых решений и планируемых комплексов мероприятий по обеспечению национальной безопасности РФ.

Изложенные результаты разработки формализованной методологической базы, включают понятийный аппарат сценарного исследования, а также функциональные схемы, отражающие разветвленный многоуровневый механизм формирования сценариев и моделирования процессов развития обстановки. Предложенный подход, реализованный на основе автоматизации процессов сценарного моделирования, является важным шагом на пути решения проблем повышения эффективности управления безопасностью сложных организационных систем. Дальнейшее развитие методологии, а также ее внедрение в практику позволит проводить многосторонний комплексный и

одновременно с этим детальный анализ альтернативных путей развития общественно-политической и социально-экономической ситуации в стране как результата реализации тех или иных решений по совершенствованию процессов управления обеспечением национальной безопасности. Это должно также способствовать не только исключению возможных ошибок, чреватых серьезными последствиями, но и повышению качества и результативности принимаемых решений в рассматриваемой предметной области.

Литература

1. Стратегия национальной безопасности Российской Федерации (утв. указом Президента Российской Федерации от 02.07.2021 г. № 400).
2. *Шульц В.Л., Кульба В.В., Чернов И.В., Шелков А.Б.* Сценарный анализ проблем управления обеспечением безопасности сложных социально-экономических систем // Управление развитием крупномасштабных систем: труды 15-й Международной конференции (MLSD'2022). – М.: ИПУ РАН, 2022. – С. 55–66.
3. *Шульц В.Л., Чернов И.В., Кульба В.В., Шелков А.Б.* Сценарное планирование в управлении обеспечением национальной безопасности: методологические основы // Национальная безопасность / nota bene. 2023. № 5. – С. 36–61.
4. *Шульц В.Л., Кульба В.В., Шелков А.Б., Чернов И.В., Тимошенко А.А.* Методы анализа влияния процессов трансформации права на развитие социально-экономической системы в условиях цифровизации: сценарный подход (постановка задачи) // Российский журнал правовых исследований. 2021. Т. 8. №1. – С. 19–36.
5. *Буланов В.Б.* Сценарный анализ развития Амурской области / В.Б. Буланов, О.А. Дашкова, О.А. Шулигина, Д.А. Кононов, И.В. Чернов. – М.: ИПУ РАН, 2009. – 143 с.
6. *Schultz, V.L., Kulba, V.V., Avdeeva, Z.K., Shelkov, A.B., Chernov, I.V.* Decision Support System on Social Stability Governance Based on Scenario Approach // International Journal of Engineering and Technology (UAE). – 2018. – Vol 7, № 2.28. – P. 240–242.
7. *Чернов И.В.* Сценарный анализ уязвимости при управлении сложными системами // Автоматика и телемеханика. 2022. № 5. – С. 133–147.
8. *Шульц В.Л.* Модели и методы анализа и синтеза сценариев развития социально-экономических систем / В.Л. Шульц, В.В. Кульба, Д.А. Кононов, С.А. Косяченко, А.Б. Шелков, И.В. Чернов. В 2-х книгах. Книга 1. – М.: Наука, 2012. – 304 с.
9. *Дранко О.И.* Управление развитием региона. Моделирование возможностей / О.И. Дранко, Д.А. Новиков, А.Н. Райков, И.В. Чернов. – М.: URSS, ООО «ЛЕНАНД», 2023. – 432 с.