УДК 338.24, 004.89, 004.942

А. В. Маслобоев, В. А. Путилов

Специфика и структура задачи информационной поддержки управления безопасностью региональных социально-экономических систем

A. V. Masloboev, V. A. Putilov

Specificity and structure of regional security control information support problem

Аннотация. Работа посвящена системному анализу проблем информационного обеспечения безопасности регионального хозяйства и методам их решения на различных стадиях жизненного цикла развития кризисных ситуаций. Рассматривается специфика и структура задач управления региональной безопасностью в экономике как объекта информационной поддержки. Сформулирован комплекс задач информационной поддержки принятия решений на трех уровнях регионального управления: стратегическом, тактическом, оперативном. Предложена единая методологическая и инструментальная база для их решения.

Abstract. The paper deals with system analysis of problems of regional economy information security and methods for their solutions at various stages of the crisis situation life-cycle. Specificity and structure of control problems of regional security in the economy as an object of information support have been considered. A set of decision-making information support problems occurred at the strategic, tactical and operational levels of regional security management has been defined. The information support problem-solving unified methodological and instrumental framework of regional security has been proposed.

Ключевые слова: региональная безопасность, управление, информационная поддержка, жизненный цикл угроз, кризисная ситуация, моделирование, информационные технологии.
Key words: regional security, control, information support, threat life-cycle, crisis situation, simulation, information technologies.

Введение

Системный анализ проблем управления региональной безопасностью показывает, что в современных условиях повышение эффективности и безопасности функционирования региональных социально-экономических систем (РСЭС), подверженных влиянию множества внутренних и внешних угроз различной природы, является одним из важнейших стратегических направлений развития национальной экономики и обороноспособности страны. Это обусловлено необходимостью обеспечивать устойчивое поступательное развитие и стабильность функционирования РСЭС в различных условиях неблагоприятного воздействия внешних и внутренних факторов как социально-экономического, природно-техногенного, геополитического характера, так и инспирированных человеком. Особенно актуальна эта проблема для арктических регионов России.

Управление региональной безопасностью заключается в создании благоприятных условий для обеспечения устойчивого поступательного развития РСЭС, подверженных воздействию динамически изменяющихся внутренних и внешних угроз различной природы. Эти условия определяются имеющейся инфраструктурой безопасности региона (информационной, правовой, транспортной, социальной и т. д.). Информационная среда региональной безопасности является одним из важнейших компонентов этой инфраструктуры, поскольку на стратегическом, тактическом и оперативном уровнях управления безопасностью региона требуется адекватная информационно-аналитическая поддержка и координация процессов принятия управленческих решений на всех этапах жизненного цикла кризисных ситуаций – от зарождения и идентификации потенциальных угроз региональной безопасности до реакции и восстановления.

Для решения проблемы управления региональной безопасностью необходимо, чтобы процессы обеспечения региональной безопасности были управляемыми. Управляемость предполагает создание многоуровневой системы управления этими процессами. Подходом, призванным повысить качество управления безопасностью региона, является реализация информационного управления развитием и функционированием РСЭС посредством создания целостной многофункциональной информационной среды региональной безопасности [1]. Под *информационным управлением* понимается механизм управления, основанный на информационно-аналитической поддержке процесса выработки и реализации управленческих решений в ситуациях, когда управляющее воздействие носит неявный, косвенный характер, и субъекту управления предоставляется информация о ситуации, ориентируясь на которую он получает возможность корректировать линию поведения объекта управления. В работе в качестве такого объекта рассматривается региональная безопасность.

Специфика задачи информационного управления региональной безопасностью

Информационно-аналитическая поддержка управления региональной безопасностью заключается в создании информационной среды (инфраструктуры) безопасности региона и поддержании ее в адекватном задачам информационного обеспечения состоянии. Для удовлетворения актуальным требованиям к информационному обеспечению региональной безопасности такая информационная среда должна быть целостной в смысле охвата всех этапов жизненного цикла угроз региональной безопасности, расширяемой и наделенной потенциалом к саморазвитию. Для создания подобных информационных сред необходимы соответствующие методы и информационные технологии получения, интеграции, анализа и обработки информации, обеспечивающие:

– формализованное представление знаний о предметной области как основы для автоматизации отдельных аспектов управления региональной безопасностью;

– логическую интеграцию и композицию разнородных информационно-вычислительных ресурсов;

– формирование и динамическое конфигурирование многоуровневых распределенных систем управления безопасностью с активными элементами и перестраиваемой структурой;

– мониторинг жизненного цикла угроз региональной безопасности;

– экспертно-имитационное моделирование развития кризисных ситуаций;

– координацию процессов принятия решений на всех уровнях управления в сфере региональной безопасности.

Информационное управление региональной безопасностью по своей структуре многофункционально и в общем случае включает в себя такие функции управления, как целеполагание, стратегическое планирование, оперативное управление, а также функции контроля, учета, мониторинга и координации. Поэтому информационное управление региональной безопасностью является сложной, многоаспектной задачей. Во-первых, это обусловлено сложностью самого объекта информационной поддержки – процессов управления региональной безопасностью. Несмотря на то, что в последние десятилетия вопросам безопасности на различных уровнях государственного управления уделялось большое внимание, в настоящее время термин "региональная безопасность" не имеет четкого определения и может трактоваться весьма широко [2; 3; 4].

Во-вторых, региональная безопасность имеет общие черты с другими видами безопасности (национальной, международной, глобальной и др.), но отличается множественностью форм проявления, учитывающих специфические особенности конкретных регионов. Регионы, являясь компонентами единой политической и социально-экономической системы страны, обладают собственной спецификой и относятся к классу слабоструктурированных сложных динамических систем. В связи с этим, проблематика информационного обеспечения безопасности развития таких сложных объектов управления, как РСЭС, во многом определяется их специфическими особенностями. Например, особенности арктических регионов определяются как их географическим положением, так и спецификой хозяйственного освоения территорий. Специфики добавляет и перегруженность территории объектами оборонно-промышленного комплекса. Эти факторы в совокупности обусловливают уязвимость РСЭС в плане возникновения разнотипных чрезвычайных и кризисных ситуаций.

В-третьих, управление жизненным циклом угроз региональной безопасности представляет собой сложный многоэтапный процесс. На каждом этапе задействованы разнотипные субъекты управления (государственные служащие, системные аналитики, менеджеры, военные, эксперты, ученые и т. д.), имеющие различную организационную подчиненность и ведомственную принадлежность. Субъекты преследуют собственные цели с учетом их сферы интересов и обладают разными компетенциями в плане решения вопросов обеспечения безопасности. Вместе с тем, процессы обеспечения безопасности компонентов региональных систем разнородны по динамике и составу участников. Субъекты управления безопасностью, вовлеченные в эти процессы, как правило, территориально распределены. Следствием этого является отсутствие, в общем случае, единого централизованного управления региональной безопасностью, структурная разнородность субъектов управления. При проецировании такой структуры и системы управления на задачи администрирования в плоскости информационного обеспечения региональной безопасности заметно сужается круг потенциально применимых архитектур информационных систем.

Разнородность и территориальная распределенность субъектов, участвующих в процессах управления региональной безопасностью, в сочетании с динамичностью их состава и параметров, создает предпосылки для того, чтобы информационная среда региональной безопасности была интероперабельной и децентрализованной. В такой ситуации, в общем случае, уже не всегда применимы архитектуры и технологии корпоративных информационных систем, ориентированные на централизованное администрирование, хранение и обработку данных. Альтернативой им являются одноранговые или *пиринговые* (от англ. peer-to-peer – "равный к равному") архитектуры, которым характерны свойства открытости и расширяемости, а также потенциал самоорганизации [5].

Для повышения эффективности функционирования децентрализованной информационной среды региональной безопасности необходимо, с одной стороны, обеспечить качественные высокоскоростные

коммуникации, а с другой – организовать адресный информационный обмен, т. е. обеспечить получение той или иной информации только заинтересованными в ней субъектами. Это позволит снизить общий объем циркулирующей в распределенной среде информации и, следовательно, уменьшить нагрузку на реализующие ее программно-технические элементы. Одним из способов решения такой задачи является организация в распределенной информационной среде виртуальных управляющих центров [6], в пределах которых концентрируется, широковещательный по сути, информационный обмен между близкими по сфере интересов, компетенциям и профилю деятельности субъектами.

Еще одним следствием разнородности и территориальной распределенности субъектов управления региональной безопасностью является технологическая и семантическая неоднородность информационной среды региональной безопасности. Для информационного управления региональной безопасностью характерна высокая степень не только технологической (использование различных форматов хранения, представления и обмена данными, разных СУБД и структур баз данных и т. д.), но и семантической разнородности информационно-вычислительных ресурсов (использование профильными ведомствами собственных тезаурусов и процедур, синонимия в именовании информационных объектов, использование различных оценочных шкал и т. п.). Вместе с тем в процессах управления региональной безопасностью участвуют специалисты из различных предметных областей, пользующиеся различной терминологической базой, использующие отличные ментальные модели одних и тех же понятий и процессов. Источником же технологической неоднородности информационно-вычислительных ресурсов является организационная разнородность субъектов управления безопасностью, которые, как правило, к моменту начала совместной деятельности уже имеют и используют свои собственные, отличные по архитектуре и используемым технологиям, информационные поддерживающие инфраструктуры. Эти особенности, зачастую, препятствуют формированию единого информационного пространства межведомственной деятельности в сфере управления региональной безопасностью. Для преодоления технологической и семантической неоднородности совместно используемых информационно-вычислительных ресурсов для задачи информационного управления региональной безопасностью необходимы соответствующие методы, технологии и программно-технические средства. Существенную помощь в решении этих проблем могут оказать мультиагентные системы, онтологии и технологии семантического веба [7].

На разных этапах жизненного цикла угроз региональной безопасности и на разных уровнях управления существенно различаются и задачи информационно-аналитической поддержки. Как следствие, спектр используемых в настоящее время методов и средств информационного управления региональной безопасностью оказывается весьма разнообразным. При этом ни одно из существующих решений не адресует проблему в комплексе. Все это повышает роль информационного управления региональной безопасностью, заключающегося не только в сборе и предоставлении информации для поддержки принятия управленческих решений в этой сфере, но и в использовании методов и средств ее предварительного анализа и обработки для координации процессов децентрализованного управления безопасностью.

Перечисленные особенности обусловливают динамичность и разнородность информационной среды региональной безопасности, необходимость в механизмах координации взаимодействия образующих ее подсистем в условиях децентрализованного управления и принятия решений. Такая среда характеризуется сетецентричностью [8] и синтезируется на базе объединения многоуровневых систем управления различными составляющими региональной безопасности. Сетецентричность предполагает сетевую структуру организационного управления с выделенными управляющими центрами. Это добавляет задаче информационного управления региональной безопасностью дополнительные, нетрадиционные для существующих научно-методических и технологических решений аспекты.

Для повышения эффективности децентрализованного управления региональной безопасностью, согласно результатам исследований [3; 8], помимо информационной поддержки принятия решений на разных уровнях управления, необходимо обеспечить координацию показателей качества функционирования элементов и подсистем РСЭС, оптимизируемых разнородными субъектами безопасности с учетом различий в их целеполагании и многокритериальности решаемых задач управления. Вместе с тем необходимость согласованного взаимодействия субъектов управления на всех этапах жизненного цикла угроз региональной безопасности в условиях пространственно-временных и ресурсных ограничений предъявляет высокие требования к качеству информационного обеспечения региональной безопасности. Для удовлетворения этим требованиям информационная среда безопасности региона должна строиться на базе технологий, обеспечивающих ее расширяемость, про-активность, способность к самоорганизации и саморазвитию, совмещению свойств открытости и информационной защищенности, а также достаточный уровень автономности и интероперабельности интегрируемых компонентов региональных информационных систем.

На основании выше сказанного, можно констатировать следующую ситуацию в сфере информационного обеспечения региональной безопасности и, через него – управления устойчивым (безопасным) развитием РСЭС в целом. С одной стороны, существует большое количество современных методов и информационных технологий, эффективно используемых изолированно друг от друга для решения ограниченного круга задач информационно-аналитической поддержки управления региональной безопасностью. С другой стороны,

использование комплексного подхода к решению обозначенной проблемы содержит в себе потенциал для повышения эффективности информационного управления в целом, который в настоящее время практически не используется.

Как объект управления и объект информационной поддержки региональная безопасность имеет ряд существенных особенностей. К ним относится:

– большое количество, территориальная распределенность, функциональная и организационная разнородность, динамичность состава субъектов управления, участвующих в процессах обеспечения комплексной безопасности развития региона;

– различная природа и неочевидный (скрытый) характер внешних и внутренних угроз региональной безопасности;

– длительный жизненный цикл и отложенность во времени результирующих воздействий угроз региональной безопасности, выражающихся в возникновении труднопрогнозируемых чрезвычайных и кризисных ситуаций;

– распределенность, технологическая, семантическая и организационная разнородность информационных ресурсов, необходимых на разных этапах жизненного цикла и уровнях принятия управленческих решений в сфере региональной безопасности;

– наличие слабо формализуемых и трудно поддающихся автоматизации начальных этапов жизненного цикла угроз региональной безопасности, включающих зарождение и развитие потенциальных угроз и опасностей, а также проведение упреждающих диагностирующих мероприятий.

Одной из ключевых особенностей региональной безопасности является организационная разнородность субъектов управления, вовлеченных в процессы обеспечения безопасности. Это обстоятельство затрудняет возможность использования для комплексной информационной поддержки управления жизненным циклом угроз региональной безопасности существующих технологий централизованных информационных систем, являющихся, как правило, основой организации функционирования распределенных ситуационно-кризисных центров, в силу того, что последние подразумевают организацию пользователей в жесткую иерархическую структуру.

Существующие подходы к информационному обеспечению региональной безопасности в основном ограничены созданием и поддержкой разного рода мониторинговых информационно-аналитических систем для ситуационных центров и веб-ресурсов, обеспечивающих субъектам управления доступ к информационно-справочным материалам и нормативным документам на основе соответствующих информационных технологий. Эти ресурсы интегрируют в себе большой объем разноплановой информации о различных объектах безопасности, угрозах, инцидентах, событиях, кризисных ситуациях, планах совместных действий, составе участников кризисного реагирования, регламентах взаимодействия и т. д. Однако чаще всего ресурсы принадлежат разным ведомствам и не связаны между собой, разнородны по технологиям реализации и семантике содержимого. Для совокупного использования ресурсов пользователь должен многократно повторять процедуры согласования доступа к интересующей его информации, регистрации и поиска данных в каждой ведомственной информационной системе в отдельности. При этом низкий уровень интероперабельности интегрируемых компонентов ведомственных информационных систем, а также автоматизации процедур поиска исполнительных ресурсов (субъектов совместной деятельности) и формирования организационных структур управления безопасностью в разнотипных кризисных ситуациях приводит к тому, что в условиях большого суммарного объема информации, необходимой для поддержки принятия оперативных и стратегических управленческих решений, практическая ценность поисковых и мониторинговых функций в особенности на ранних этапах жизненного цикла угроз региональной безопасности существенно снижается.

Таким образом, проблема информационной поддержки сетецентрического управления региональной безопасностью требует комплексного решения четырех взаимосвязанных задач:

1) задача обработки, анализа и интеграции семантически и организационно разнородной распределенной информации о состоянии компонентов региональных систем;

2) задача формализации экспертных знаний с последующим синтезом на их основе новых знаний об исследуемых объектах или процессах для поддержки принятия управленческих решений;

3) задача координации (согласования) взаимодействия между субъектами регионального управления в процессе принятия стратегических, оперативных и тактических решений с учетом информации, поступающей в режиме реального времени;

4) задача формирования единой информационной среды (инфраструктуры) региональной безопасности.

Решение первой и второй задачи является основой для решения третьей и четвертой задачи.

Комплексная информационная поддержка процессов управления региональной безопасностью на различных этапах развития кризисных ситуаций позволяет повысить качество принимаемых решений на стратегическом, тактическом и оперативном уровнях управления, с одной стороны, и сократить временные и материальные затраты на реализацию антикризисных мероприятий – с другой. Вместе с тем качественная информационно-аналитическая поддержка обеспечивает сокращение продолжительности жизненного

цикла угроз региональной безопасности за счет уменьшения времени отклика (реакции) на возникающие кризисные ситуации уже на начальных этапах их развития в динамически изменяющихся условиях.

Возможность действовать на опережение, быстрое реагирование и адаптация к динамике внешней среды, а значит и качественное информационное обеспечение в особенности важны для эффективного управления региональной безопасностью, которое характеризуется многофункциональностью и структурной сложностью, с одной стороны, и слабой изученностью, высокой неопределенностью и отложенностью результатов – с другой.

Структура задачи информационного управления региональной безопасностью

Разнородность и динамичность состава участников процессов управления региональной безопасностью, а также многообразие выполняемых ими функций обусловливают структурную сложность и многоаспектность проблемы информационного управления региональной безопасностью. В связи с этим, важнейшим условием ее успешного решения является четкое понимание структуры и содержания составляющих ее подзадач. В общем случае для решения этой проблемы необходимо как методическое, так и информационное обеспечение.

Методическое обеспечение управления региональной безопасностью представляет собой совокупность как уже существующих, так и разрабатываемых в настоящее время методов и средств информационного мониторинга и целенаправленной обработки "сырых" и архивных данных, в том числе информации, поступающей в режиме реального времени. Методическое обеспечение, в основном, включает в себя методы и средства поддержки принятия решений, а также средства автоматизации отдельных аспектов управления региональной безопасностью.

Информационное обеспечение управления региональной безопасностью: для эффективной информационной поддержки процессов принятия решений на разных уровнях управления в сфере региональной безопасности необходимы соответствующие информационные ресурсы и сервисы. Информационные ресурсы играют роль своего рода "сырого материала", из которого путем адекватной переработки на основе соответствующих сервисов можно получать новые данные и знания, необходимые для обоснованного выбора и претворения в жизнь оперативных и стратегических решений по управлению региональной безопасностью в кризисных ситуациях.

К таким базовым информационным ресурсам относятся:

– различные базы данных ведомственных информационных систем, содержащие информацию об объектах и показателях безопасности, потенциальных угрозах и сценариях их развития, инцидентах, событиях, кризисных ситуациях, типовых планах организации антикризисных мероприятий, составе участников кризисного реагирования, регламентах взаимодействия и т. д.

– веб-ресурсы, обеспечивающие информационно-справочную поддержку и удобный унифицированный распределенный доступ к данным;

– средства телекоммуникаций, обеспечивающие абстрагирование от территориальной привязки субъектов управления и ресурсов безопасности.

Информационное обеспечение не ограничивается простым накоплением все больших и больших объемов разноплановой информации о потенциально возможных чрезвычайных и кризисных ситуациях и угрозах безопасности, а представляет собой набор различных информационных, облачных и веб-сервисов, реализующих:

– тренажерно-моделирующие комплексы;

– средства формирования имитационных моделей сложных процессов, протекающих в РСЭС;

– средства интеграции, обработки и анализа информации;

– средства мониторинга, прогнозирования и сценарного анализа социально-экономического развития;

– средства информационно-аналитической поддержки деятельности организационных структур управления региональной безопасностью и т. д.

Задача информационного управления региональной безопасностью также может быть структурирована в соответствии с тремя основными компонентами инфраструктуры безопасности региона, к которым относятся:

– ресурсы безопасности – организационные, административные, финансовые, информационные и другие;

– инфраструктура безопасности, обеспечивающая условия для реализации эффективного управления региональной безопасностью;

– антикризисное управление, обеспечивающее формирование планов антикризисных мероприятий и их реализацию.

В соответствии с этим, задача информационного управления региональной безопасностью включает несколько аспектов:

– создание информационных ресурсов для поддержки управления и принятия решений в сфере региональной безопасности – баз данных, словарей и прочих ресурсов, имеющих отношение к задачам управления безопасностью РСЭС, а также удобных средств оперативного распределенного доступа к ним;

– создание средств информационно-аналитической поддержки антикризисного управления, прежде всего средств интеллектуальной поддержки принятия решений на базе когнитивного и имитационного моделирования процессов управления региональной безопасностью;

– создание информационной инфраструктуры региональной безопасности, обеспечивающей формирование проблемно-ориентированных групп субъектов управления безопасностью (организационных структур управления безопасностью) и соответствующих информационных ресурсов и сервисов, предназначенных для поддержки отдельно взятой организационной структуры безопасности в рамках локализации (предотвращения) возникшей кризисной ситуации.

Структуризацию задачи информационного управления региональной безопасностью можно произвести также в соответствии с задачами, возникающими как на разных уровнях управления региональной безопасностью, так и на разных фазах жизненного цикла развития кризисных ситуаций. В работе предложено выделять четыре уровня управления региональной безопасностью: стратегический, оперативно-стратегический, оперативно-тактический и тактический. Оперативно-стратегический и оперативно-тактический уровни образуют в совокупности оперативный уровень управления региональной безопасностью. В силу очевидных и весьма существенных различий во внутренней структуре и локальной целенаправленности процессов, протекающих на разных стадиях развития кризисных ситуаций, существенно отличаются и требования к средствам информационной поддержки на различных уровнях управления и принятия решений в сфере региональной безопасности.

Перечислим основные задачи информационной поддержки, решаемые на разных уровнях управления региональной безопасностью.

На *стратегическом уровне* управления решаются следующие задачи:

1) управление знаниями о разнородных объектах и процессах обеспечения безопасности;
2) управление компетенциями субъектов безопасности, участвующих в этих процессах;
3) формирование организационных структур управления безопасностью в кризисных ситуациях;
4) формирование сети центров организационного управления региональной безопасностью.

Основной задачей на этом уровне является формирование организационных структур управления безопасностью, обеспечивающих допустимый с точки зрения стоимостных затрат, пространственно-временных и ресурсных ограничений уровень эффективности предотвращения и ликвидации кризисных ситуаций.

Оперативно-стратегический уровень управления региональной безопасностью включает следующие задачи информационной поддержки:

1) ситуационный и сценарный анализ, оценка результативности реализации антикризисных мероприятий;
2) синтез траекторий и реализация управления "точно в срок";
3) реконфигурация сети центров управления региональной безопасностью.

Оперативно-тактический уровень управления предполагает решение следующих задач:

1) информационный мониторинг потенциальных угроз и опасностей;
2) оценка качества и эффективности организационных структур управления безопасностью;
3) реконфигурация организационных структур управления безопасностью в кризисных ситуациях.

На *тактическом уровне* решаются задачи, связанные непосредственно с управлением кризисными ситуациями, выбором участников (акторов) и исполнительных ресурсов, необходимых для локализации конкретных угроз безопасности или кризисных ситуаций, а также формированием и согласованием планов совместных действий. Основной задачей на этом уровне управления является анализ профиля деятельности субъектов управления безопасностью. Это необходимо для определения соответствия их компетенций и возможностей участия в предотвращении текущих или прогнозируемых кризисных ситуаций. При этом спецификации кризисных ситуаций должны быть декомпозированы на подзадачи и распределены между субъектами управления безопасностью. В рамках этой задачи осуществляется подбор (композиция) компетенций субъектов управления, представляющих собой совокупность предоставляемых ими ресурсов и услуг (сервисов), которые могут быть использованы в процессах обеспечения региональной безопасности.

На концептуальном уровне жизненный цикл угроз региональной безопасности представляет собой совокупность взаимосвязанных этапов: 1) зарождение угрозы; 2) развитие угрозы; 3) проникновение в РСЭС; 4) проникновение в критическую область развития РСЭС; 5) инициализация угрозы; 6) воздействие угрозы; 7) регенерация (восстановление) РСЭС с возможным порождением новой угрозы.

Угрозы порождают разнотипные кризисные ситуации. Под *кризисной ситуацией*, согласно [9], понимается обстановка на определенной территории, сложившаяся в результате техногенной аварии, опасного природного явления, террористического акта, социально-экономического, геополитического или межнационального конфликта, которая повлекла за собой социальную нестабильность, человеческие жертвы, значительные материальные потери, угрожающие жизни и безопасности граждан, нормальной деятельности государственных и общественных институтов. Качественное описание и классификация типов региональных кризисных ситуаций представлены в работе [4].

Жизненный цикл развития кризисной ситуаций содержит следующие фазы: 1) идентификация угроз безопасности; 2) планирование антикризисных мероприятий; 3) кризисное реагирование; 4) ликвидация последствий (восстановление).

В соответствии с логикой развития кризисных ситуаций в социально-экономической сфере, процессы управления региональной безопасностью должны охватывать весь комплекс проблем регионального развития, а система информационной поддержки (управления) - функционировать в следующих трех основных режимах: 1) стационарном (режим стабильности); 2) чрезвычайном (локализация развивающихся кризисных ситуаций); 3) постчрезвычайном (ликвидация последствий кризисных ситуаций).

Наиболее сложным является начальный период зарождения и развития кризисных ситуаций. Этот этап является плохо формализуемым и трудно прогнозируемым в силу неочевидного (скрытого) характера угроз и их проявлений, в связи с этим на этой начальной стадии жизненного цикла задача информационной поддержки выглядит наиболее расплывчато. На этапе зарождения угрозы, зачастую, даже не существует конкретного объекта информационной поддержки.

На этой начальной стадии жизненного цикла облик кризисной ситуации еще не сформировался, и главная задача информационного обеспечения заключается в создании наиболее адекватной среды для противодействия развитию потенциальных угроз и опасностей. Общеизвестным подходом к решению этой задачи, согласно [10], является использование методов и средств информационного и проблемного мониторинга социально-экономической обстановки в регионе с привлечением экспертного сообщества, на основе социологических опросов, сценарного анализа, анализа архивных статистических данных, а также с применением современных информационно-коммуникационных технологий, социальных сетей и т. д. Роль информационной поддержки на данном этапе достаточно высока: современные компьютерные технологии обеспечивают сбор, автоматизированную обработку и анализ больших объемов разноплановой информации для выявления потенциальных угроз и опасностей регионального развития и поддержки принятия адекватных сложившейся ситуации управленческих решений на основе этой информации. Вместе с тем обеспечивается возможность создания виртуальных анализаторов (мониторов) – аналогов центров управления в кризисных ситуациях и центров мониторинга социально-экономического развития на базе мониторинговых информационно-аналитических систем, облачных, агентных и веб-технологий. Эти виртуальные аналоги, по сравнению со своими реальными объектами, хотя и теряют отдельные аспекты своей функциональности вследствие виртуализации, но взамен обеспечивают на порядки большие информационные и аналитические возможности, экономию ресурсов и снижение затрат, увеличивают потенциальное количество субъектов управления и экспертов, участвующих в процессах обеспечения региональной безопасности, обеспечивают интеграцию и обработку коллективных экспертных знаний с последующим синтезом на их основе новых знаний, что крайне важно для реализации эффективного информационного управления региональной безопасностью в разнородных кризисных ситуациях.

В настоящее время информационная поддержка данной фазы жизненного цикла, как правило, сводится в основном к созданию и поддержанию в актуальном состоянии различных баз и картотек данных ведомственных информационных систем и мониторинговых информационно-аналитических систем, используемых в составе ситуационно-кризисных центров. Эти ресурсы содержат семантически и организационно разнородную, часто слабоструктурированную информацию об источниках потенциальных угроз и опасностей, кризисных ситуациях и их параметрах, планах антикризисных мероприятий, показателях безопасности, критически важных объектах и процессах обеспечения безопасности. То же самое можно констатировать и в отношении специализированных информационно-справочных веб-ресурсов. Как правило, все эти средства информационной поддержки используются изолированно друг от друга и принадлежат разным ведомствам (субъектам управления безопасностью). Подобные информационно-вычислительные ресурсы, несомненно, играют важную положительную роль в информационной поддержке управления региональной безопасностью на ранних стадиях развития кризисных ситуаций. Однако их использование подразумевает активный поиск информации со стороны субъектов управления безопасностью. Наличие у последних достаточно сильной мотивации к поиску необходимой информации для принятия эффективных управленческих решений появляется чаще всего уже после зарождения угрозы и претворения кризисной ситуации в жизнь. Таким образом, ведомственные информационные системы обеспечивают, в большей степени, поддержку второго этапа жизненного цикла угроз региональной безопасности, когда осуществляется целенаправленный предметный поиск субъектов совместной деятельности, ресурсов и путей разрешения уже зафиксированных, развивающихся кризисных ситуаций.

Эффективность использования информационно-вычислительных ресурсов ведомственных информационных систем для задач управления региональной безопасностью может быть увеличена за счет обеспечения совместного использования территориально распределенных разнородных информационных баз и частичной автоматизации обработки содержащихся в них данных. Современным средством решения задачи автоматизированной интеллектуализированной обработки разнородной информации из различных источников являются агентные технологии [11]. Программные агенты, будучи способными к целенаправленным активным действиям от лица своих владельцев, позволяют автоматизировать не только предметный поиск

информации в разнородных территориально рассредоточенных источниках, но и обеспечивают возможность оценки потенциальных угроз региональной безопасности в многомерном пространстве признаков, а также поиск решений в условиях нечеткой постановки задачи, создавая тем самым возможность частичной автоматизации процессов управления региональной безопасностью в кризисных ситуациях.

Важной проблемой, которую необходимо решить для успешного использования агентных технологий автоматизированной обработки информации, является семантическая неоднородность информационных ресурсов, необходимых для задач информационного управления региональной безопасностью. Информационные ресурсы одной предметной области могут содержать отличающиеся внешне термины, понятия, сущности, которые, тем не менее, могут быть семантически связанными, близкими по смыслу, и, наоборот, имея одинаковые названия, могут нести абсолютно разную смысловую нагрузку. Эффективным средством описания и анализа семантики разнородных ресурсов являются сетевые модели представления знаний [12], в частности онтологии [13] и концептуальное моделирование предметной области [14].

На остальных этапах жизненного цикла угроз региональной безопасности в основном решаются две группы задач информационной поддержки:

1) задачи планирования и оперативного управления процессами обеспечения безопасности в кризисных ситуациях;

2) задачи моделирования и автоматизации процессов управления кризисными ситуациями.

Различные задачи информационной поддержки определяют и различие используемых на разных этапах жизненного цикла угроз региональной безопасности информационных технологий, методов и средств компьютерного моделирования, баз данных, веб-технологий, технологий интеллектуальных информационных систем, средств поддержки принятия решений и т. д.

Соотношение фаз развития кризисных ситуаций и этапов жизненного цикла угроз региональной безопасности с технологиями информационной поддержки приведено на рисунке.

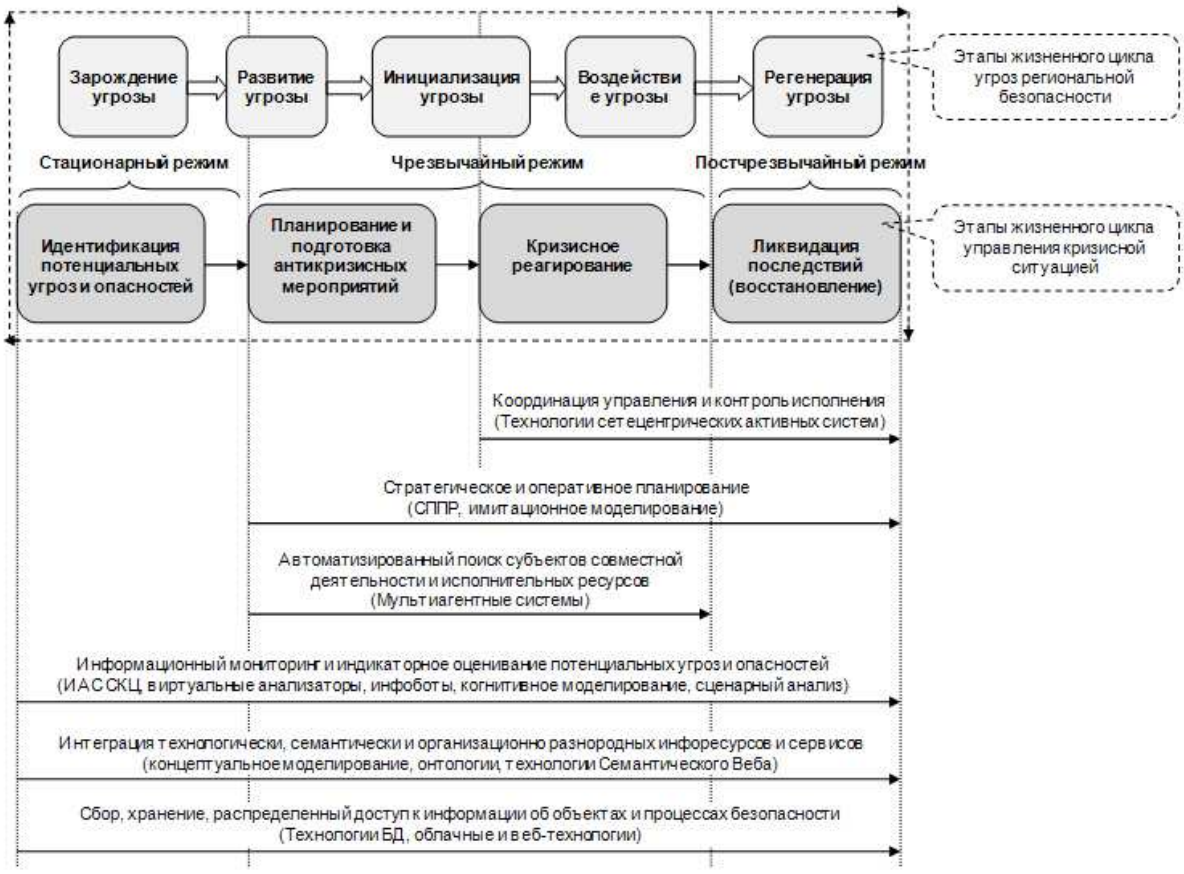

Рис. Этапы жизненного цикла и технологии информационной поддержки

Одной из ключевых проблем на сегодняшний день является согласованное использование и интеграция существующих разработок для сквозного информационного управления жизненным циклом угроз региональной безопасности на всех его этапах – от зарождения и развития потенциальных угроз и опасностей до предотвращения и ликвидации возникших кризисных и чрезвычайных ситуаций.

Таким образом, задачи информационного обеспечения региональной безопасности пронизывают все уровни управления (стратегический, оперативно-стратегический, оперативно-тактический и тактический)

и могут быть выделены в отдельную категорию. Сетецентрическое информационное управление региональной безопасностью является одним из наименее исследованных подходов в управлении безопасностью региональных социально-экономических систем. Это перспективная предметная область, появление которой обусловлено прогрессом как в развитии новых организационных форм управления сложными слабоструктурированными системами различной природы, так и прогрессом в сфере информационно-коммуникационных технологий, которые позволяют на сегодняшний день говорить о возможности решения проблемы автоматизации процессов сетецентрического управления безопасностью развития региональных социально-экономических систем.

Заключение

В ходе исследований получены следующие результаты:

1. Проведен системный анализ проблем информационного обеспечения региональной безопасности с целью определения требований к разработке средств информационно-аналитической поддержки, обеспечивающих повышение эффективности децентрализованного управления безопасностью РСЭС в динамически изменяющихся условиях.

2. Предложены структуризация задач информационной поддержки управления региональной безопасностью в соответствии со специфическими особенностями предметной области исследования, методы и средства комплексного решения этих задач на всех уровнях управления.

Результаты исследований смогут найти применение при реализации "Стратегии развития Арктической зоны Российской Федерации и обеспечения национальной безопасности на период до 2020 года" на территории Мурманской области в части создания новых информационных технологий для задач управления региональным развитием и комплексной безопасностью РСЭС.

Работа выполнена при поддержке РФФИ (проект № 15-07-04290-а).

Библиографический список

1. Маслобоев А. В. Мультиагентная информационно-аналитическая среда поддержки управления региональной безопасностью "Безопасный Виртуальный Регион" // Научно-технический вестник информационных технологий, механики и оптики. 2013. № 4 (86). С. 128–138.

2. Загребнев С. Региональная безопасность в системе национальной безопасности Российской Федерации // Власть. 2010. № 10. С. 90–92.

3. Маслобоев А. В., Путилов В. А., Сютин А. В. Многоуровневая рекуррентная модель иерархического управления комплексной безопасностью региона // Научно-технический вестник информационных технологий, механики и оптики. 2014. № 6 (94). С. 163–170.

4. Управление региональной безопасностью на основе сценарного подхода / В. Л. Шульц [и др.]. М. : ИПУ РАН, 2014. 163 с.

5. Сухорослов О. В. Пиринговые системы: концепция, архитектура и направления исследований // Труды Института системного анализа РАН. Проблемы вычислений в распределенной среде: прикладные задачи. М. : РОХОС, 2004. С. 7–43.

6. Маслобоев А. В. Виртуальные когнитивные центры как интеллектуальные системы для информационной поддержки управления региональной безопасностью // Научно-технический вестник информационных технологий, механики и оптики. 2014. № 2 (90). С. 167–170.

7. Расселл С., Норвиг П. Искусственный интеллект. Современный подход. М. : Вильямс, 2007. 1408 с.

8. Маслобоев А. В., Путилов В. А., Сютин А. В. Координация в многоуровневых сетецентрических системах управления региональной безопасностью: подход и формальная модель // Научно-технический вестник информационных технологий, механики и оптики. 2015. Т. 15, № 1. С. 130–138.

9. Ямалов И. У. Моделирование процессов управления и принятия решений в условиях чрезвычайных ситуаций. М. : БИНОМ. Лаборатория знаний, 2007. 288 с.

10. Олейник А. Г., Путилов В. А. Организация информационно-аналитической структуры поддержки управления региональным развитием // Труды Института системного анализа РАН: Прикладные проблемы управления макросистемами. 2010. Т. 59. С. 175–192.

11. Wooldridge M. An Introduction to MultiAgent Systems. Second Edition. John Wiley & Sons, 2009. 484 p.

12. Гаврилова Т. А., Хорошевский В. Ф. Базы знаний интеллектуальных систем. СПб. : Питер, 2000. 384 с.

13. Ломов П. А., Шишаев М. Г. Интеграция данных на основе онтологий для обеспечения информационной поддержки управленческих решений // Труды Института системного анализа РАН. М. : Книжный дом "ЛИБРОКОМ", 2008. Т. 39. С. 159–173.

14. Кузьмин И. А., Путилов В. А., Фильчаков В. В. Распределенная обработка информации в научных исследованиях. Л. : Наука, 1991. 304 с.

References

1. Masloboev A. V. Mul'tiagentnaja informacionno-analiticheskaja sreda podderzhki upravlenija regional'noj bezopasnost'ju "Bezopasnyj Virtual'nyj Region" [Multi-agent information and analytical system "Secured Virtual Region" for regional security management support] // Nauchno-tehnicheskij vestnik informacionnyh tehnologij, mehaniki i optiki. 2013. N 4 (86). P. 128–138.
2. Zagrebnev S. Regional'naja bezopasnost' v sisteme nacional'noj bezopasnosti Rossijskoj Federacii [Regional security in the national security system of the Russian Federation] // Vlast'. 2010. N 10. P. 90–92.
3. Masloboev A. V., Putilov V. A., Syutin A. V. Mnogourovnevaja rekurrentnaja model' ierarhicheskogo upravlenija kompleksnoj bezopasnost'ju regiona [A hierarchical control multilevel model of complex regional security] // Nauchno-tehnicheskij vestnik informacionnyh tehnologij, mehaniki i optiki. 2014. N 6 (94). P. 163–170.
4. Upravlenie regional'noj bezopasnost'ju na osnove scenarnogo podhoda [Scenario-based approach for regional security control] / V. L. Shul'c [i dr.]. M. : IPU RAN, 2014. 163 p.
5. Suhoroslov O. V. Piringovye sistemy: koncepcija, arhitektura i napravlenija issledovanij [P2P-systems: conception, architecture and research directions] // Trudy Instituta sistemnogo analiza RAN. Problemy vychislenij v raspredelennoj srede: prikladnye zadachi. M. : ROHOS, 2004. P. 7–43.
6. Masloboev A. V. Virtual'nye kognitivnye centry kak intellektual'nye sistemy dlja informacionnoj podderzhki upravlenija regional'noj bezopasnost'ju [Virtual cognitive centers as intelligent systems for management information support of regional security] // Nauchno-tehnicheskij vestnik informacionnyh tehnologij, mehaniki i optiki. 2014. N 2 (90). P. 167–170.
7. Rassell S., Norvig P. Iskusstvennyj intellekt. Sovremennyj podhod [Artificial intelligence: A modern approach]. M. : Vil'jams, 2007. 1408 p.
8. Masloboev A. V., Putilov V. A., Sjutin A. V. Koordinacija v mnogourovnevyh setecentricheskih sistemah upravlenija regional'noj bezopasnost'ju: podhod i formal'naja model' [Coordination in multilevel network-centric control systems of regional security: Approach and formal model] // Nauchno-tehnicheskij vestnik informacionnyh tehnologij, mehaniki i optiki. 2015. T. 15, N 1. P. 130–138.
9. Yamalov I. U. Modelirovanie processov upravlenija i prinjatija reshenij v uslovijah chrezvychajnyh situacij [Simulation of control and decision-making processes within the emergency situations]. M. : BINOM. Laboratorija znanij, 2007. 288 p.
10. Olejnik A. G., Putilov V. A. Organizacija informacionno-analiticheskoj struktury podderzhki upravlenija regional'nym razvitiem [Information and analytical structure organization of regional development management support] // Trudy Instituta sistemnogo analiza RAN: Prikladnye problemu upravlenija makrosistemami. 2010. T. 59. P. 175–192.
11. Wooldridge M. An Introduction to MultiAgent Systems. Second Edition. John Wiley & Sons, 2009. 484 p.
12. Gavrilova T. A., Horoshevskij V. F. Bazy znanij intellektual'nyh sistem [Knowledge bases of intelligent system]. SPb. : Piter, 2000. 384 p.
13. Lomov P. A., Shishaev M. G. Integracija dannyh na osnove ontologij dlja obespechenija informacionnoj podderzhki upravlencheskih reshenij [Ontology-based data integration for managerial decision-making information support] // Trudy Instituta sistemnogo analiza RAN. M. : Knizhnyj dom "LIBROKOM", 2008. T. 39. P. 159–173.
14. Kuz'min I. A., Putilov V. A., Fil'chakov V. V. Raspredelennaja obrabotka informacii v nauchnyh issledovanijah [Distributed information processing in the scientific research]. L. : Nauka, 1991. 304 p.

Сведения об авторах

Маслобоев Андрей Владимирович – Институт информатики и математического моделирования технологических процессов КНЦ РАН, канд. техн. наук, доцент, ст. науч. сотрудник; e-mail: masloboev@iimm.ru

Masloboev A. V. – Institute for Informatics and Mathematical Modeling of Technological Processes KSC RAS, Cand. of Tech. Sci., Associate Professor, Senior Research Fellow; e-mail: masloboev@iimm.ru

Путилов Владимир Александрович – Институт информатики и математического моделирования технологических процессов КНЦ РАН, д-р техн. наук, профессор, директор; e-mail: putilov@iimm.ru

Putilov V. A. – Institute for Informatics and Mathematical Modeling of Technological Processes KSC RAS, Dr. of Tech. Sci., Professor, Director; e-mail: putilov@iimm.ru