УДК 004.056

Синергетический подход к обеспечению устойчивости функционирования автоматизированных систем специального назначения

Захарченко Р. И., Королев И. Д., Саенко И. Б.

Аннотация. *Интеграция разнотипных информационных систем государственной информационной системы (ГИС), в том числе и автоматизированных систем специального назначения Федеральных органов исполнительной власти (далее по тексту АС СН), через информационно-телекоммуникационные сети общего пользования (ИТКС ОП) привело к доступности АС СН через киберпространство. Функционирование АС СН в условиях целенаправленных информационно-технических воздействий (ИТВ), особенности АС СН как объекта управления, а также неопределенность знаний об окружающей среде и действующих факторах, целей и динамики их изменений, привели к необходимости учета в методологии и технологиях обеспечения устойчивости функционирования совокупностей факторов, ранее не имевших места.* ***Целью работы*** *является разработка синергетического подхода управления процессами обеспечения устойчивости функционирования АС СН в условиях кибернетического противоборства, а также способов его практической реализации.* ***Результат и его новизна.*** *В статье рассматривается синергетический подход к построению адаптивной системы поддержки принятия решения (СППР) АС СН, функционирующей в условиях ИТВ в киберпространстве. Предлагаемый подход базируется на комбинации методов многокритериальной полезности в соответствии с критериями оптимальности, присущими процедурам принятия решения с учетом текущей целевой функции и в данных условиях.* ***Практическая значимость*** *представленного подхода состоит в том, что может быть использован в перспективных СППР для повышения адекватности управления устойчивостью функционирования АС СН, а также обоснования новых форм и способов ведения кибернетического противоборства.*

Ключевые слова: *киберпространство, информационно-технические воздействия, управление устойчивостью, синергетические свойства, СППР.*

Актуальность

Высокая степень автоматизации управления и объединение разнотипных информационных систем (ИС), в том числе и автоматизированных систем специального назначения Федеральных органов исполнительной власти (далее по тексту АС СН), через информационно-телекоммуникационные сети общего пользования (ИТКС ОП) привело к формированию глобального информационного пространства и новой среды его функционирования – киберпространства [1, 2]. Феномен наличия и успешного функционирования данного объекта при отсутствии явных признаков соответствующей теории его возникновения и развития не соответствует известным способам создания сложных систем [1, 3].

Библиографическая ссылка на статью:
Захарченко Р. И., Королев И. Д., Саенко И. Б. Синергетический подход к обеспечению устойчивости функционирования автоматизированных систем специального назначения // Системы управления, связи и безопасности. 2018. № 4. С. 207–225. URL: http://sccs.intelgr.com/archive/2018-04/11-Zakharchenko.pdf

Reference for citation:
Zakharchenko R. I., Korolev I. D., Saenko I. B. Synergistic approach to the management of sustainable functioning of the special purpose automatic systems. *Systems of Control, Communication and Security*, 2018, no. 4, pp. 207–225. Available at: http://sccs.intelgr.com/archive/2018-04/11-Zakharchenko.pdf (in Russian).

Следовательно, возникает необходимость его описания. При этом речь идет о нематериальных ресурсах, искусственных воздействиях и виртуальной среды их существования, рассмотрение которых порождает ряд новых де-факто сложившихся, но юридически незакрепленных в РФ терминов и их определений. Обзор и авторское видение терминологии в данной области представлен в работах [2, 4, 5].

Доступность через киберпространство АС СН ставит обеспечение национальной безопасности в зависимость от степени ее защищенности и напрямую зависит от владения соответствующим среде оружием, степени его эффективности, методов использования и средств защиты от него [1-5], т.е. созданы предпосылки возникновения противоборства в киберпространстве.

При ведении кибернетического противоборства используется новый вид оружия – кибернетическое оружие, вырабатывающее информационно-технические воздействия (ИТВ), которое не является оружием в классическом понимании, т.е. не осуществляют физическое поражение объекта атаки, а переводит его автоматизированную систему управления (АСУ) в критический режим функционирования [5]. Нарушение функционирования АСУ может привести к различным эффектам: от временной потери управления в АС СН до физического разрушения потенциально опасных (критических) объектов, находящихся под ее управлением. По оценке зарубежных экспертов, эффект целевого применения кибернетического оружия на ИС сравним с эффектом применения оружия массового поражения [1, 3]. Следовательно, функционирование АС СН в новой среде – киберпространстве, порождает новые уязвимости и угрозы, и требует разработки нового инструментария обеспечения безопасности АС СН, под которой понимается состояние ее защищенности, обеспечивающее ее устойчивое функционирование в условиях компьютерных атак [6].

Обеспечение качественного решения задач, связанных с обеспечением устойчивости функционирования АС СН в рамках единого информационного пространства в современных условиях невозможно без широкого внедрения автоматизированной обработки данных на основе АСУ. При этом очевидно, что для компенсации угроз устойчивости функционирования АС СН необходимо ее рассматривать как композицию взаимосвязанных функций, сетей и технологий, что существенно усложняет задачу управления устойчивостью функционирования АС СН.

Разработка и совершенствование АСУ АС СН связаны с целым комплексом нерешенных научно-технических проблем [7]. Эти обстоятельства указывают на значительную важность решения проблемы разработки новых подходов, моделей и методов, способных обеспечить устойчивое функционирование АС СН.

Синергетический подход к управлению процессами обеспечения устойчивости АС СН

Управление процессами обеспечения устойчивостью функционирования АС СН основывается на знаниях о состоянии объектов управления, состоянии среды функционировании и оказываемых воздействиях [8, 9]. Неотъемлемым

элементом таких систем управления является подсистема поддержки принятия решения, которая в сложных системах выступает в роли самостоятельной системы поддержки принятия решения (СППР). Возможности по управлению устойчивостью функционирования АС СН напрямую зависят от возможностей СППР [10-12], способности ее обеспечить лица принимающие решения (ЛПР) в качественно сбалансированной форме информацией, характеризующей реальное и прогнозируемые состояния АС СН, и обеспечить обоснованный выбор траектории достижения цели в условиях противоборства в киберпространстве.

Анализ подходов к сетецентрическому управлению подобного класса ИС, выполненный в работе автора [13], показывает, что необходимо качественное изменение принципов управления и способов организации информационного обеспечения процессов управления. Одним из таких инструментариев качественного повышения эффективности обеспечения процессов управления может стать новый метод на основе использования синергетического эффекта.

Построение СППР, позволяющей обеспечить адекватное управление АС СН в условиях противоборства в киберпространстве, невозможно без анализа не только связей отдельных АС СН в целом (ведомственной АС СН) и на появляющихся при этом эмерджентных свойствах, но и выявлении причин их возникновения, т.е. синергетических свойств.

Рассмотрение синергетических свойств АС СН позволит повысить управляемость системы за счет повышения согласованности управляющих воздействий с собственными тенденциями системы, а также варьированием мощностью связей частей в целом (позволяет как укреплять, так и ослаблять уже существующие связи) [7, 8, 12].

Обоснованием целесообразности рассмотрения синергетических свойств в активных сложных технических системах является установленный факт, что кооперация многих подсистем какой-либо системы подчиняется одним и тем же принципам их функционирования независимо от природы подсистем [14]. Формализация этих принципов позволяет по-новому подойти и к проблеме адекватного управления процессами обеспечения устойчивости функционирования АС СН с учетом присущих ей ограничений [7, 8, 11].

Синергетические свойства вытекают из таких основных характеристик АС СН как функциональность, адаптивность и жизнестойкость. Все элементы АС СН обладают уникальными возможностями, свойствами и функциями, что приводит систему в процессе функционирования в состояние перманентных изменений. К примеру, такое свойство АС СН как жизнестойкость выражается в неуклонном следовании цели функционирования. Функциональность АС СН заключается в процессе развития собственной уникальности и наращивания своих возможностей, а также развитии вариативности при их реализации. Адаптивность, как третье свойство сложной системы, это способность отдельных ее элементов сосуществовать в гармонии с самими собой и с окружающим миром, т.е. изменять свои функции и структуру в зависимости от складывающейся ситуации и условий внешней среды [12, 14].

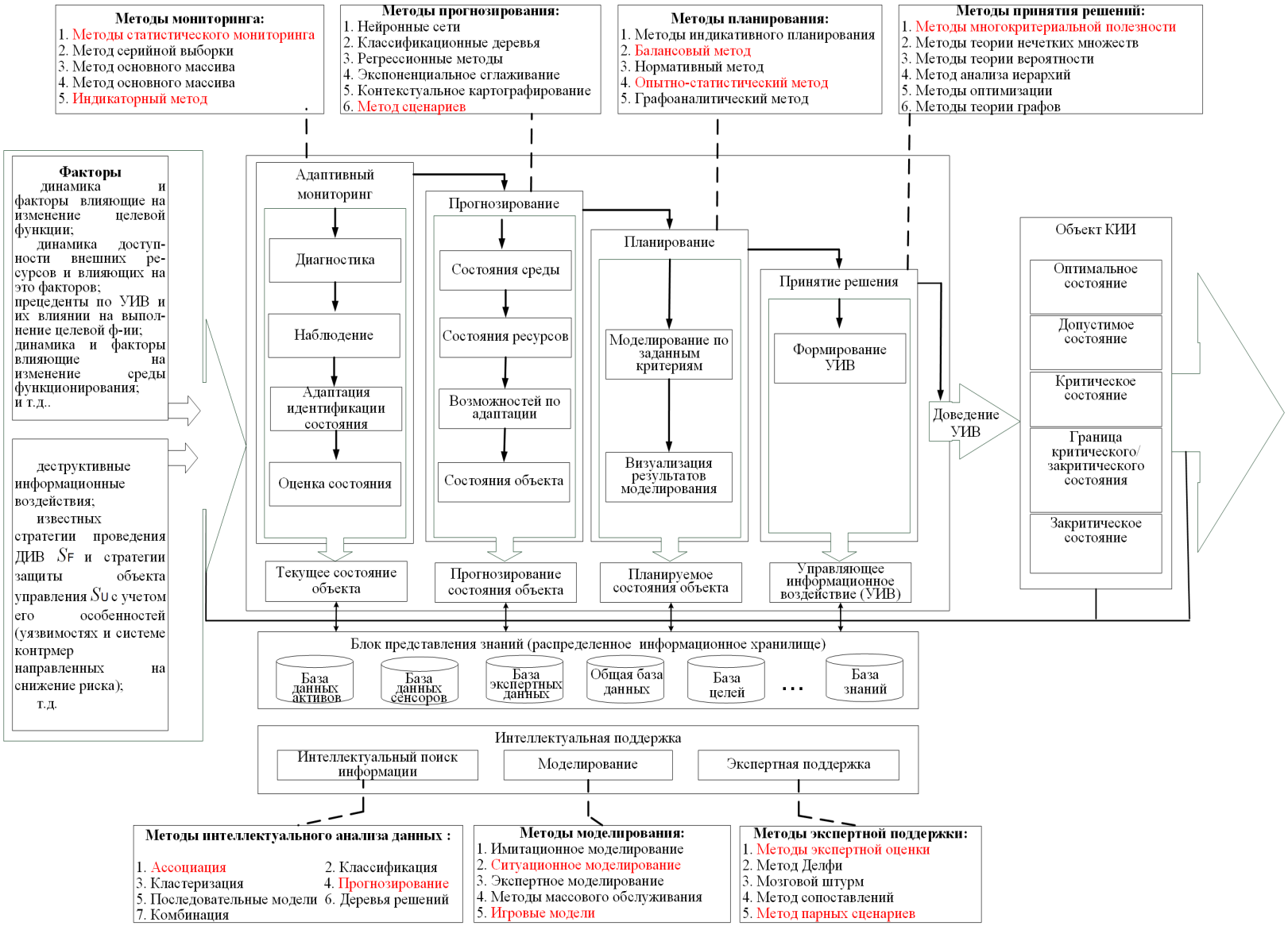

Рис. 1. Обобщенная модель адаптивной СППР АС СН и предлагаемые для применения в ней методы

Проведенный сравнительный анализ методов построения СППР [12-16] показал, что отдельно взятые методы обладают как преимуществами, так и недостатками. Соответственно только в продуманной комбинации методов, применяемых в СППР, может эмерджентность и синергетический эффект, когда дополнительность сведет к минимуму частные недостатки отдельных методов и позволит автоматизировано решать сложные задачи управления рис. 1.

Признаковое пространство управления процессами обеспечения устойчивости функционирования АС СН

Обеспечение устойчивости функционирования АС СН невозможно без наличия полной оперативной информации о состоянии всех ее элементов, оказываемых на них воздействий и внешних и внутренних ограничений, что требует разработки соответствующей модели, представленной на рис. 2.

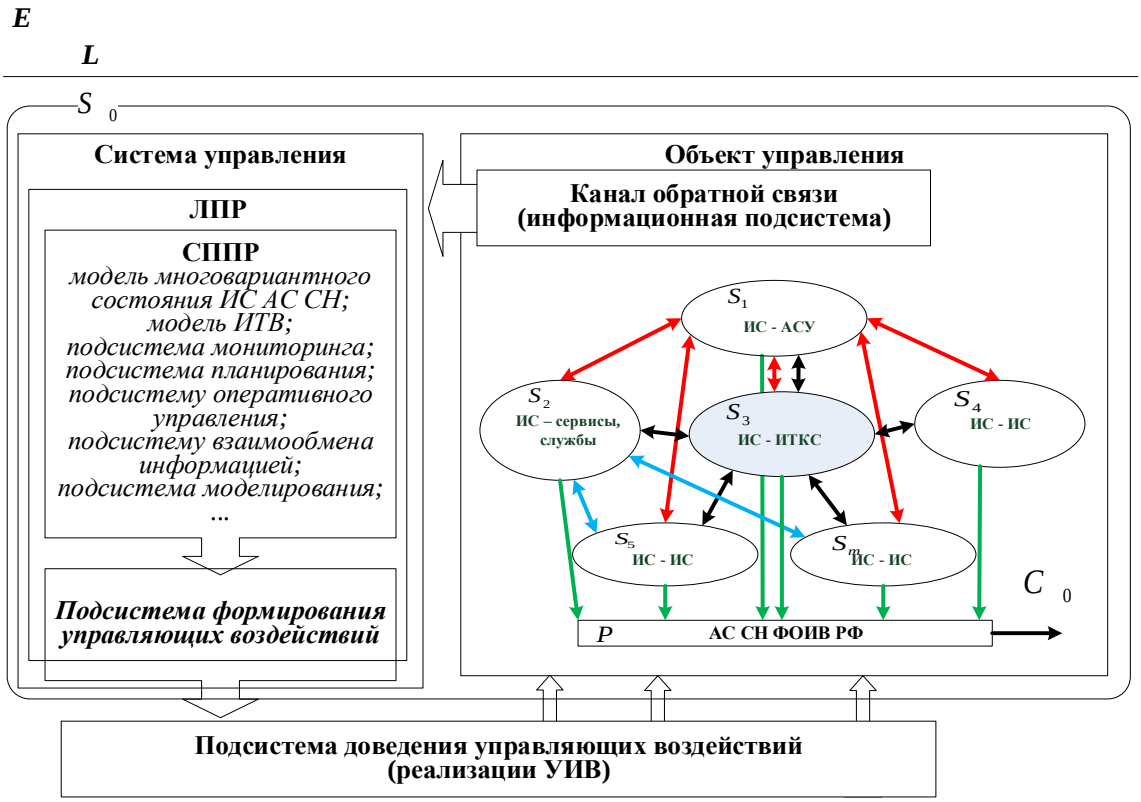

Рис. 2. Модель обеспечения устойчивости АСУ СН в киберпространстве

Разрабатываемая модель должна учитывать проявления не только статических и динамических воздействий среды (E) на множество отдельных информационных систем ИС (S_m), объединенных единой целью (C_0) по признаку существования в кластер, связанных между собой каналами связи.

Архитектура АС СН имеет внутреннюю структуру – взаиморасположение элементов (отдельных ИС) и связей, – задающую устойчивость и воспроизведение выполнения целевой функции. Отдельные информационные системы, в свою очередь, состоят из n элементов (технических средств обработки инфор-

мации, различающихся свойствами, проявляющимися при взаимодействии), объединенных связями (стрелками – линии передачи данных, управляющих воздействий или других информационных потоков) и вступающих в определенные отношения *O* между собой и средой функционирования, чтобы осуществить процесс *P* (последовательность действий для изменения или поддержания состояния) и выполнить свою целевую (целевые) функцию – C_n.

Формализованное представление разрабатываемой модели информационного пространства EIS_0 для функционирования АС СН S_0 можно выразить как:

$$EIS_0 = <S_0, I, L, C_0, E, P>,$$

где: EIS_0 – киберпространство АС СН (S_0);

I – модель киберпространства, зафиксированная в форме информационного ресурса;

L – характер информационного взаимодействия АС СН (S_0) и отдельных ИС;

C_0 – единая цель информационного взаимодействия АС СН в киберпространстве (*E*);

E – модель киберпространства для АС СН (S_0) и отдельных ИС $\{S_1,...,S_n\}$;

P – стратегия (план действий) для изменения или поддержания состояния (S_0).

Таким образом, АС СН представляет собой систему, состоящую из большого числа технических средств обработки информации (ТСОИ), программных компонентов и подсистем, сложным образом взаимодействующих между собой. Подобные системы в теории управления называются сложными техническими объектами и описываются через взаимодействующие технические или технологические процессы, в результате которых происходит превращение входных потоков в продукцию [11]. При этом внешняя среда и ЛПР не являются элементами технического объекта, а под техническим объектом понимается «совокупность упорядоченно взаимодействующих элементов, обладающая свойствами, не сводящимися к свойствам отдельных элементов, и предназначенная для выполнения определенных полезных технологических функций» [10, 11].

Многочисленные технические системы, созданные человеком, обладают рядом общих свойств, признаков и структурных особенностей [8, 12, 15]. Это позволяет считать АС СН единой группой объектов, обладающих следующими свойствами:

- состоят из частей, элементов, то есть имеют структуру;
- созданы для каких-то целей, то есть выполняют целевые функции;
- элементы имеют связи друг с другом, соединены в подсистемы и организованы в некотором пространстве и времени;
- группа объектов обладает определенным качеством, неравным простой сумме свойств составляющих ее подсистем (эмерджентностью).

Взаимосвязь многочисленных подсистем и их элементов образуют свойство – *сложность*. Сложные технические системы состоят из большего числа

элементов. Технические системы, как правило, являются большими с огромным количеством разнородных связей для выполнения заданной целевой функции (функций). Эти связи создают структурную иерархию технической системы.

В работах [16] слабо формализуемые технические системы описаны с позиций «компонентного подхода», где выделены следующие признаки:

– многоуровневая иерархия подсистем и элементов внутри подсистем;
– множественность математического описания;
– различные виды неопределенности;
– присутствие синергетического эффекта, приводящего к многовариантности состояний подсистем и их элементов (рис. 3).

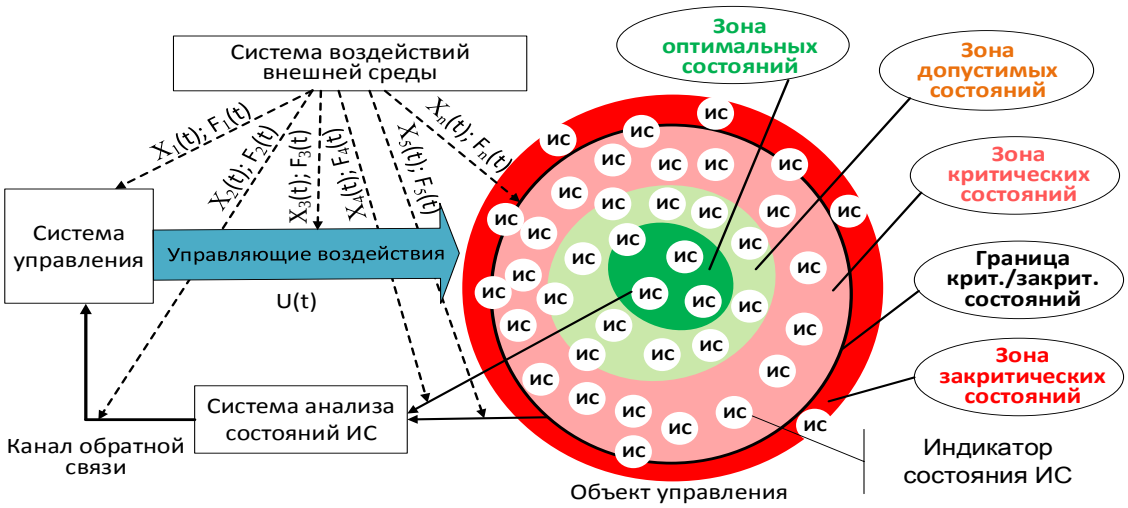

Рис. 3. Обобщенная модель многовариантного состояния АС СН

Возникновение эффекта многовариантности состояний АС СН в процессе функционирования обусловлено ее особенностями как объекта управления и необходимостью учета неопределенности информации о состоянии объекта, характеристиках его входных и выходных потоков, а также неопределенности знаний о внешней среде и воздействующих факторах [5].

Для обеспечения устойчивости функционирования АС СН в данных условиях АСУ должна компенсировать воздействия, направленные на нарушение устойчивости функционирования, путем поддержания (достижения) заданных значений функционирования отдельных элементов (ИС) и АС СН в целом.

Формализованное представление процессов обеспечения устойчивости функционирования АС СН в условиях ИТВ неразрывно связано с выполнением им целевой функции, достижение которой может быть описано кортежем вида:

$$Y = \langle S, C, V, T, R, Z, G, Q \rangle,$$

где: Y – множество выходных данный АС СН;

S – множество конфигураций АС СН, определяющих ее текущую структуру и множество функциональных связей;

C – множество целей функционирования АС СН;

V – множество параметров состояния АС СН;

T – множество моментов времени наблюдения элементов АС СН;

R – множество ресурсов АС СН;

$Z = <F, X, U>$ – множество воздействий на АС СН;

F – множество деструктивных воздействий на АС СН;

X – множество воздействий внешней среды на АС СН;

U – множество управляющих воздействий на АС СН;

Q – множество показателей качество функционирования АС СН;

G – критерии оценки состояния функционирования АС СН:

$G > 0{,}9$ – область оптимальных состояний (система исправна);

$0{,}9 \leq G < 0{,}7$ – область допустимых состояний (система неисправна, но работоспособна);

$0{,}7 \leq G < 0{,}5$ – область критических состояний (система неисправна, не работоспособна, но правильно функционирует);

$0{,}5 \leq G < 0{,}3$ – граница областей критических/закритических состояний (система неисправна, неработоспособна, неправильно функционирует, подлежит восстановлению);

$G \leq 0{,}3$ – область закритических состояний (система неисправна, неработоспособна, неправильно функционирует, не подлежит восстановлению).

Указанные выше характеристики отдельных ИС (АС СН в целом) и воздействующие на них факторах можно с достаточной для практики точностью представить конечным множеством параметров – индикатором состояния ИС (АС СН).

Таким образом, любое из возможных состояний объекта управления можно описать через индикатор его состояния [18], а затем с использованием методики оценки определить степень достижения текущей цели по соответствующим критериям.

Подсистема адаптивного мониторинга АС СН

В качестве эффективного средства предметной организации информации о состоянии АС СН целесообразно осуществить её "модельное" представление как организованных знаний, несущих функционально необходимую и достаточно обоснованную системную информацию об объекте мониторинга (рис. 4). При этом динамика изменения целей и воздействий различной природы на объект мониторинга в процессе функционирования происходит непредвиденным образом, и адекватной модели, описывающей состояние объекта мониторинга, в нужный момент может не оказаться, вследствие чего возникает необходимость выполнять адаптацию процедур мониторинга.

Процесс синтеза модели объекта мониторинга связан с последовательной комбинированной многоуровневой адаптацией процедур мониторинга непосредственно в ходе их проведения. Для этого в процесс адаптации процедур мониторинга необходимо учитывать специфические условия их реализации и соответствие критериям оптимальности, что позволит описать текущее состояния АС СН адекватно целям СППР и с учетом влияния внешних и внутренних, конструктивных и деструктивных информационных воздействий.

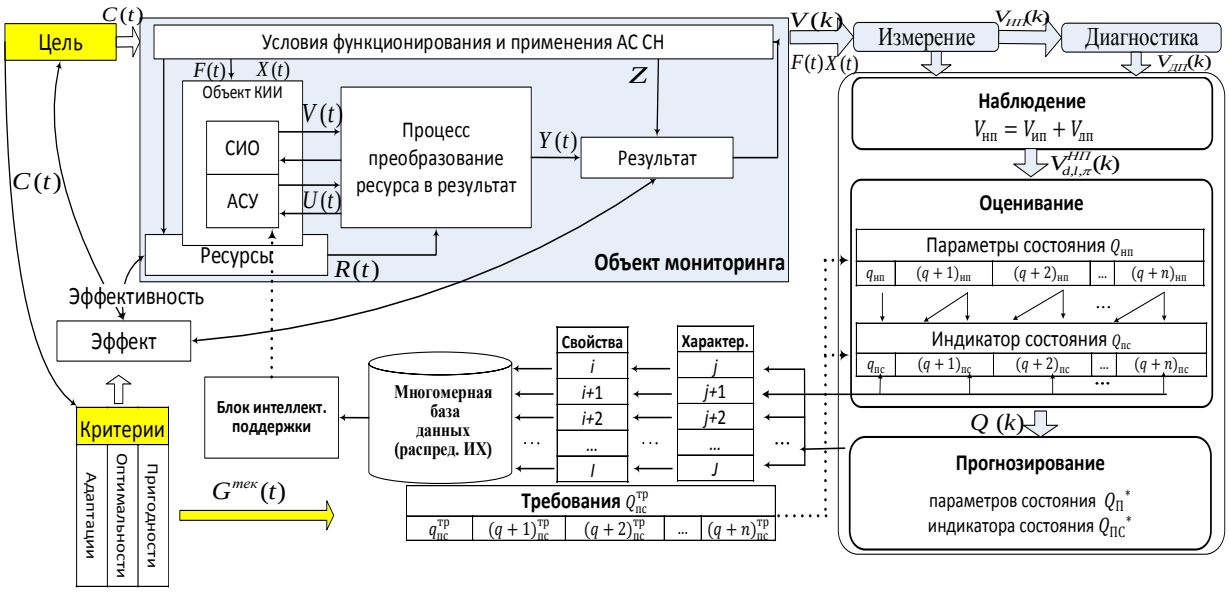

Рис. 4. Модель адаптивного мониторинга АС СН

Адаптация процедур мониторинга должна выражаться в возможности выбора наиболее приемлемых режимов выполнения процедур мониторинга АС СН.

Выбор режима реализации процедур наблюдения, оценивания и прогнозирования состояния АС СН должен осуществляться в зависимости от изменяющихся целей функционирования и соответствовать текущим задачам управления АС СН с целью обеспечения заданного уровня устойчивости функционирования, что обуславливает необходимость учета:

- текущих внешних и внутренних факторов:
- известных стратегий проведения ИТВ и стратегий обеспечения устойчивости функционирования АС СН;
- динамики изменения текущих целей функционирования АС СН и управления ими;
- динамики доступности необходимых на реализацию процедур мониторинга ресурсов в рамках цикла управления устойчивостью функционирования АС СН и влияющих на это факторов;
- условий обстановки, т.е. наличия воздействующих факторов (факторов ТЭ, ЖЦ и эксплуатационных факторов), определяющих состояние отдельных сетевых сервисов, отдельных ИС и АС СН в целом;
- уровня управления устойчивостью функционирования или размера сегмента АС СН, затронутого изменениями состояния.

Таким образом, при адаптации процессов мониторинга должна решаться задача оптимизации, позволяющая минимизировать набор параметров, подлежащих контролю, за счет максимизации полезности добываемых данных (повышения информативности) при обеспечении заданного критериального порога полноты с учетом доступности необходимых на реализацию процедур мониторинга ресурсов и установленных ограничений на остальные характеристики мониторинга АС СН [18,19].

Полученное в ходе выполнения адаптивного мониторинга описание фактического состояния АС СН позволяет выполнить оценку ее способности выполнять целевые функции, достижение которой может быть описано кортежем вида:

$$Q_{AM}^{K} =< Y(k); D; V_{d,l,\pi}^{H}; R_d; S; C; G; Q_d >,$$

где: Q_{AM} – оценка текущего состояния АС СН в процессе адаптивного мониторинга АС СН на k шаге мониторинга;

$Y(k)$ – множество выходных данные АС СН на k шаге мониторинга;

D – множество сетевых сервисов АС СН;

$V_{d,l,\pi}$ – множество наблюдаемых параметров сервиса d;

R_d – ресурсы необходимые для функционирования сервиса d;

S – множество конфигураций АС СН определяющих ее структуру и множество функциональных связей;

C – множество целей функционирования АС СН;

G – множество критериев способности выполнять целевую функцию в текущей ситуации.

Q_d – множество показателей качества функционирования сетевого сервиса d.

Концептуальный подход и базирующийся на нем метод оценки способности АС СН выполнять целевые функции представлен авторами в более ранней работе [9]. Суть его заключается в декомпозиции АС СН на отдельные ИС, а их, в свою очередь, на сетевые сервисы. Оценка отдельных сервисов с учетом коэффициентов связанности и степени важности выполняемых в данный момент ими функций позволяет оценить отдельные ИС, а на основе полученных оценок и АС СН в целом.

Иными словами, система адаптивного мониторинга выполняет ряд взаимосвязанных задач, на основании решения которых получаются исходные данные, необходимые для принятия решения о состоянии (оптимальное, допустимое, критическое) АС СН для выполнения определенных функций в данный момент времени и в данных условиях.

Подсистема представления эмпирических данных

Результат сбора параметров, описывающих фактическое состояние АС СН в непрерывной динамике и с учетом всей совокупности влияющих на нее факторов, представляет собой поток данных, который содержит достаточно разнородные и несогласованные данные: состояния среды функционирования, оказываемые воздействия, а также данные, характеризующие работу входящих в состав АС СН технических средств обработки информации, программного обеспечения, сервисов, служб, коммутационного оборудования и т.д.

При накоплении этих статистических данных получаются большие массивы разнородной информации о процессах, явлениях, событиях, объектах, субъектах и т.п., пополняемые непрерывно в режиме реального времени [19, 20].

На данный момент, существует достаточно большое количество различных подходов к анализу данных, начиная от традиционных, использующих методы математической статистики, и заканчивая методами интеллектуальной обработки данных. Каждый из методов требует представление собранных данных в определенном формате для возможности их дальнейшей обработки и получения результатов в виде, понятном для человека.

Для применения методов математической статистики информация должна быть представлена в виде однородных данных, а методы интеллектуальной обработки данных позволяют обрабатывать достаточно разнородные и несогласованные данные [18, 20].

Анализ опыта применения технологий интеллектуального анализа данных [21] позволяет утверждать, что для их реализации требуется специально спроектированные информационные хранилища, отличительной чертой которых является то, что разнородная, несогласованная информация представляется в сбалансированном виде, а затем структурированная и неструктурированная информация обрабатывается совместно, как единое целое.

Качество представляемой информации после аналитической обработки СППР будет определяться, прежде всего, объемом накопленных эмпирических данных и применяемым методом интеллектуального анализа данных [9, 16, 18].

Необходимость накопления эмпирических данных в специально спроектированном информационном хранилище способствует формированию ведомственного (для отдельного Федерального органа исполнительной власти) электронного, постоянно пополняющегося архива поведенческой активности самых различных объектов, подлежащих мониторингу, от ТСОИ отдельных ИС до АС СН в целом, для чего предлагается построить соответствующую многомерную базу данных (рис. 5).

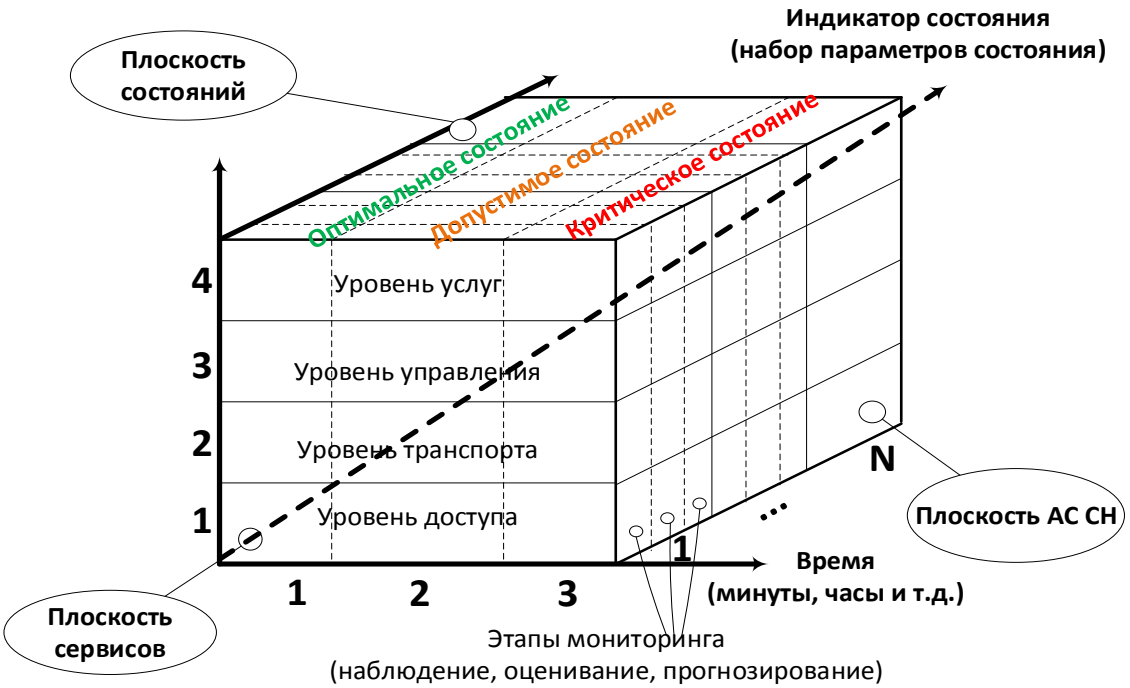

Рис. 5. Модель представления информации о состоянии АС СН в многомерной базе данных (МБД)

Формализованное представление разрабатываемой модели представления эмпирических данных в многомерной базе данных ($М_{мбд}$) АС СН можно выразить кортежем следующего вида:

$$М_{мбд} = <П_с, П_{сер}, П_{ассн}, П_Т>,$$

где: $М_{мбд}$ – модель представления эмпирических данных в многомерной базе данных;

$П_с = <D, V_d, R_d, T, G_d, Q_d>$ – плоскость состояний;

$П_{сер} = <S, \Lambda, B_{mnoa}, D, T, R_d>$ – плоскость сервисов;

$П_{ассн} = <S, B_{mnoa}, R, T, C, K>$ – плоскость АС СН;

$П_Т$ – плоскость времени;

D – множество сервисов АС СН;

V_d – множество параметров состояния d-сервиса;

R_d – ресурсы необходимые для функционирования d-сервиса;

T – множество моментов времени наблюдения элементов АС СН;

G_d – критерии способности выполнять d-сервисом целевую функцию;

Q_d – множество показателей качества функционирования сетевого сервиса d;

S – множество состояний;

C – множество целей функционирования АС СН;

K – множество каналов связи, соединяющие объекты АС СН;

B_{mnoa} – иерархическое представление АС СН;

Λ – информационная структура АС СН.

Использование технологии информационного хранилища с аналитической обработкой информации на базе многомерной базы данных позволяет [18, 19]:

- проводить самые различные и сколь угодно подробные классификации той или иной совокупности внешних и внутренних, конструктивных и деструктивных информационных воздействий, фактических выходных данных и параметров, описывающих систему и действия человеческой составляющей по самым разнообразным признакам. Такие классификации обеспечивают точное понимание взаимосвязи тех или иных характеристик любой АС СН, тем самым обеспечив анализ как эмерджентных, так и синергетических свойств;
- осуществлять многомерный статистический математический анализ. Этот анализ позволяет находить корреляцию между самыми различными параметрами, характеристиками, событиями и т.п. Теоретические модели отвечает на вопрос – почему, а затем, выявив причинно-следственные закономерности, позволяют формировать рекомендации о порядке действий;
- выполнять прогнозирование на основе классификаций и выявленной корреляционной связи факторов, определять наиболее целесообразный способ воздействия для того, чтобы один набор факторов, характеризующий текущее состояние АС СН (параметры состояния, должностное лицо его использующее, разные события и т.п.), был преобразован в заданный с прогнозированием необходимого для перехода времени.

Таким образом, реализация концепции информационного хранилища, построенного на МБД, позволит обеспечить СППР необходимой информацией для обеспечения адекватного управления устойчивостью функционирования АС СН с использованием методов многокритериальной полезности, осуществив полный охват всех решаемых ей задач, включая традиционно трудные для автоматизации задачи планирования и прогнозирования.

Выводы

По итогам представленных материалов статьи, обобщая выше сказанное, можно сделать следующие основные выводы.

1. Интеграция разнотипных ИС АС СН через киберпространство порождает новые уязвимости и угрозы и ставит обеспечение национальной безопасности в зависимость от степени их защищенности. При этом под безопасностью АС СН, понимается состояние защищенности АС СН, обеспечивающее ее устойчивое функционирование в условиях компьютерных атак.

Очевидно, что для компенсации данных угроз необходимо внедрение соответствующей системы управления устойчивостью функционирования, которая будет рассматривать АС СН как композицию взаимосвязанных функций, сетей и технологий, что существенно усложняет задачу управления устойчивостью. Основой системы управления устойчивостью является СППР.

2. Обеспечение устойчивости функционирования АС СН в сложных АСУ возможно только при комплексном решении научных задач управления процессами устойчивости с позиций системного подхода.

Применение системного подхода и соответствующих принципов к проведению исследований обеспечивает научность постановки и решения проблемы обеспечения устойчивости функционирования АС СН, ее декомпозицию на частные задачи исследования и агрегирование полученных частных результатов. Очевидно, что при этом комплексность методов исследования порождает качественно новый научный подход – синергетический.

Рассмотрение синергетических свойств АС СН позволит повысить управляемость системы за счет повышения согласованности управляющих воздействий с собственными тенденциями системы, а также варьированием мощностью связей частей в целом (позволяет как укреплять, так и ослаблять уже существующие связи).

3. Анализ тенденций развития и построения перспективных СППР позволил предложить способы практической реализации предлагаемого синергетического подхода.

Сравнительный анализ методов построения СППР показал, что только в продуманной комбинации методов, применяемых в СППР, может возникнуть эмерджентность и синергетический эффект, когда дополнительность сведет к минимуму частные недостатки отдельных методов и позволит автоматизированно решать сложные задачи практики принятия решения:

– для сбора параметров, описывающих состояния АС СН, необходимо построить соответствующую подсистему мониторинга, адекватную целям СППР и учитывающую влияние внешних и внутренних, кон-

структивных и деструктивных информационных воздействий, что требует применение метода адаптации процессов мониторинга. Полученное описание фактического состояния АС СН позволяет выполнить оценку способности АС СН выполнять целевые функции в данный момент времени и в данных условиях.

- построение СППР, способной осуществить полный охват всех решаемых ею задач, включая традиционно трудные для автоматизации задачи планирования и прогнозирования, требует применения методов интеллектуального анализа данных. Качество представляемой информации после аналитической обработки в СППР будет определяться, прежде всего, объемом накопленных эмпирических данных и применяемым методом интеллектуального анализа данных.
- необходимость накопление эмпирических данных в специально спроектированном информационном хранилище способствует формированию постоянно пополняющегося архива поведенческой активности самых различных объектов: от ТСОИ отдельных ИС до АС СН в целом.
- выбор стратегии, позволяющей достигнуть текущую цель, что требует формализации ситуации принятия решения – построения математической модели проблемной ситуации и использованием методов многокритериальной полезности.

Литература

1. Стародубцев Ю. И., Бегаев А. Н., Давлятова М. А. Управление качеством информационных услуг. – СПб.: Изд-во Политехнического университета, 2017. – 454 с.

2. Глобальная безопасность в цифровую эпоху: стратагемы для России. – М.: ВНИИгеосистем, 2014. – 394 с.

3. Бедрицкий А. В. Информационная война: концепции и их реализация в США / под ред. Е.М. Кожокина – М.: РИСИ, 2008. – 187 с.

4. Макаренко С. И., Чукляев И. И. Терминологический базис в области информационного противоборства // Вопросы кибербезопасности. 2014. № 1 (2). С. 13-21.

5. Захарченко Р. И., Королев И. Д, Мирошниченко Е. Л. Противоборство в киберпространстве: концептуальные основы и терминологический базис // Труды V Международной НПК-2017. – Краснодар, 2017. – С. 112-131.

6. О безопасности критической информационной инфраструктуры РФ. Федеральный закон РФ от 26.07.2017 № 187-ФЗ // Официальный интернет-портал правовой информации [Электронный ресурс]. 2018. – URL: http://publication.pravo.gov.ru/Document/View/0001201707260023 (дата обращения: 02.11.2018).

7. Фисун А. П., Касилов А. Г., Фисенко В. Е., Минаев В. А., Афанасьев В. В., Митяев В. В., Фисун Р. А., Джевага К. А., Кожухов С. А. Развитие методологических основ информатики и информационной

безопасности систем. Депонированная рукопись № 1165-В2004 07.07.2004. – М.: ВИНИТИ, 2004. – 253 с.

8. Новиков Д. А., Петраков С. Н. Курс теории активных систем. – М.: СИНТЕГ, 1999. – 104 с.

9. Захарченко Р. И., Королев И. Д. Методика оценки устойчивости функционирования объектов КИИ, функционирующих в киберпространстве // Наукоемкие технологии в космических исследованиях Земли. 2018. Т. 10. № 2. С. 52-61.

10. Цыпкин Я. З. Адаптация и обучение в автоматических системах. – М.: Наука, 1968. – 400 с.

11. Теория систем и системный анализ в управлении организациями: Справочник. – М.: Финансы и статистика, 2006. – 848 с.

12. Волкова В. Н., Денисов А. А. Основы теории систем и системного анализа. – СПб.: Изд-во СПбГТУ, 1977. – 512 с.

13. Макаренко С. И. Информационное противоборство и радиоэлектронная борьба в сетецентрических войнах начала XXI века. Монография. – СПб.: Наукоемкие технологии, 2017. – 546 с.

14. Заде Л. А. Основы нового подхода к анализу сложных систем и процессов принятия решений. – М.: Знание, 1974. – С. 5-49.

15. Саламатов Ю. П. Система законов развития техники (основы теории развития технических систем): учебное пособие. – Красноярск: Institute of Innovative Design, 1996. – 136 с.

16. Бочков М. В., Комарович В. Ф., Саенко И. Б. Модель адаптивной защиты информации от НСД в условиях информационного противоборства // Научно-технический сборник. № 4. – СПб.: ВУС, 2002. – С. 21-25.

17. Коцыняк М. А., Кулешов И. А., Кудрявцев М. А., Лаута О. С. Киберустойчивость информационно-телекоммуникационной сети. Монография. – СПб.: Бостон-спектр, 2015. – 150 с.

18. Захарченко Р. И., Саенко И. Б. Система поддержки принятия решения автоматизированной системы управления связи на основе организации информационного хранилища с аналитической обработкой данных // Труды академии: Научно-технический сборник № 82. – СПб.: ВАС, 2013. – С.110-119.

19. Щербатов И. А., Проталинский И. А. Сложные слабоформализуемые многокомпонентные технические системы // Управление большими системами: сборник статей. 2013. № 45. С. 30-46.

20. Макаренко С. И. Информационное оружие в технической сфере: терминология, классификация, примеры // Системы управления, связи и безопасности. 2016. № 3. С. 292-376.

21. Малинецкий Г. Г., Потапов А. Б. Современные проблемы нелинейной динамики. – М.: Эдиториал УРСС, 2000. – С.336.

References

1. Starodubtsev Yu. I., Bugaev A. N., Davlyatova M. A. *Upravlenie kachestvom informacionnyh uslug* [Management quiality of information services].

Saint-Petersburg, Publishing house of Polytechnic University, 2017. 454 p. (in Russian).

2. *Global'naya bezopasnost' v cifrovuyu ehpohu: stratagemy dlya Rossii* [Global security in the digital age: stratagems for Russia]. Moscow, Vniigeosystem publ., 2014. 394 p. (in Russian).

3. Bedritsky A. V. *Informacionnaya vojna: koncepcii i ih realizaciya v SSHA* [Information warfare: concepts and their implementation in the United States]. Moscow, The Russian Institute of Strategic Research, 2008. 187 p. (in Russian).

4. Makarenko S. I., Chuklyaev I. I. The Terminological basis in the information conflict area. *Voprosy kiberbezopasnosti*, 2014, vol. 2, no. 1, pp. 13-21 (in Russian).

5. Zakharchenko R. I., Korolev I. D, Miroshnichenko E. L. Protivoborstvo v kiberprostranstve: konceptual'nye osnovy i terminologicheskij bazis [Confrontation in cyberspace: a conceptual framework and a terminological basis]. *Proceedings of V International SPC-2017*, Krasnodar, Kuban state University, 2017, pp. 112-131 (in Russian).

6. The federal law of July 26, 2017 no. *187-FZ «About the security of the critical information infrastructure of the Russian Federation»*. Available at: http://publication.pravo.gov.ru/Document/View/0001201707260023 (accessed 2 November 2018) (in Russian).

7. Fisun A. P., Kasilov A. G., Fisenko V. E., Minaev V. A., Afanasev V. V., Mityaev V. V., Fisun R. A., Dzhevaga K. A., Kozhuxov S. A. *Razvitie metodologicheskix osnov informatiki i informacionnoj bezopasnosti sistem* [Development of methodological basics of Informatics and information security systems]. Deponirovannaya rukopis № 1165-v2004 07.07.2004. Moscow, All-Russian Institute of scientific and technical information, 2004. 253 p. (in Russian).

8. Novikov D. A., Petrakov S. N. *Kurs teorii aktivnyx sistem* [Theory of active systems]. Moscow, Sinteg Publ., 1999. 104 p. (in Russian).

9. Zakharchenko R. I., Korolev I. D. Metodika otsenki ustoychivosti funktsionirovaniya ob'ektov KII, funktsioniruyushchikh v kiberprostranstve [Technique for assessing the sustainability of the functioning of KII facilities operating in cyberspace]. *H&ES Research*, 2018, vol. 10, no. 2, pp. 52-61 (in Russian).

10. Cypkin Ya. Z. *Adaptaciya i obuchenie v avtomaticheskix sistemax* [Estimation of stability of functioning of critical information infrastructure of Federal Executive authorities]. Moscow, Nauka publ., 1968. 400 p. (in Russian).

11. *Teoriya sistem i sistemnyj analiz v upravlenii organizaciyami: spravochnik* [Systems theory and systems analysis in management of organizations: Handbook]. Moscow, Finansy i statistika publ., 2006. 848 p. (in Russian).

12. Volkova V. N., Denisov A. A. *Osnovy teorii sistem i sistemnogo analiza.* [Fundamentals of the theory of systems and system analysis]. Saint-Petersburg, Spbgtu publ., 1977. 512 p. (in Russian).

13. Makarenko S. I. *Informatsionnoe protivoborstvo i radioelektronnaia borba v setetsentricheskikh voinakh nachala XXI veka*. Monografiia [Information warfare and electronic warfare to network-centric wars of the early XXI century.

Monography]. Saint-Petersburg, Naukoemkie Tekhnologii Publ., 2017. 546 p. (in Russian).

14. Zade L. A. *Osnovy novogo podxoda k analizu slozhnyx sistem i processov prinyatiya reshenij* [Fundamentals of a new approach to the analysis of complex systems and decision-making processes.]. Moscow, Znanie publ., 1974. pp. 5-49 (in Russian).

15. Salamatov Yu. P. *Sistema zakonov razvitiya texniki (osnovy teorii razvitiya texnicheskix sistem)* [System of the laws of development of technics (the basics of the theory of technical system evolution)]. Krasnoyarsk, Institute of innovative design publ., 1996. 136 p. (in Russian).

16. Bochkov M. V., Komarovich V. F., Saenko I. B. Model adaptivnoj zashhity informacii ot nsd v usloviyax informacionnogo protivoborstva [Model of adaptive protection of information from unauthorized access in the information warfare]. *Nauchno-tekhnicheskij sbornik* [Scientific and technical collection], Saint-Petersburg, Military School of Communication publ., 2002, no. 4, pp. 21-25 (in Russian).

17. Kocynyak M. A., Kuleshov I. A., Kudryavcev M. A., Lauta O. S. *Kiberustojchivost informacionno-telekommunikacionnoj seti. Monografiya* [Cyberactivist information and telecommunications network. Monography]. Saint-Peterburg, Boston-spektr publ., 2015. 150 p. (in Russian).

18. Zaxarchenko R. I., Saenko I. B. Sistema podderzhki prinyatiya resheniya avtomatizirovannoj sistemy upravleniya svyazi na osnove organizacii informacionnogo xranilishha s analiticheskoj obrabotkoj dannyx [Decision-making support system automation communication management system based on the organization of information storage with analytical Robot data]. *Trudy akademii: Nauchno-texnicheskij sbornik* [Proceedings of the Academy: Scientific and technical collection], Saint-Petersburg, Military academy of communications publ., 2013, no. 82, pp. 110-119 (in Russian).

19. Shherbatov I. A. Protalinskij O. M. Slozhnye slaboformalizuemye mnogokomponentnye texnicheskie sistemy [Poorly formalized complex multicomponent technical systems]. *Upravlenie bolshimi sistemami*, 2013, no. 45, pp. 30-46 (in Russian).

20. Makarenko S. I. Information Weapon in Technical Area – Terminology, Classification and Examples. *Systems of Control, Communication and Security*, 2016, no. 3, pp. 292-376. Available at: http://sccs.intelgr.com/archive/2016-03/11-Makarenko.pdf (accessed 21 November 2018) (in Russian).

21. Malineckij G. G., Potapov A. B. *Sovremennye problemy nelinejnoj dinamiki* [Modern problems of nonlinear dynamics]. Moscow, Editorial URSS publ., 2000. 336 p. (in Russian).

Статья поступила 4 июня 2018 г.

Информация об авторах

Захарченко Роман Иванович – кандидат технических наук. Докторант. Краснодарское высшее военное училище. Область научных интересов: управление сложными инфокоммуникационными системами специального назначения, моделирование функционирования автоматизированных систем управления специального назначения в условиях кибернетического противоборства. E-mail: romanzakharchenko@yandex.ru

Королев Игорь Дмитриевич – доктор технических наук, профессор. Профессор. Краснодарское высшее военное училище. Область научных интересов: управление сложными инфокоммуникационными системами специального назначения, моделирование функционирования автоматизированных систем управления специального назначения в условиях кибернетического противоборства. E-mail: pi_korolev@mail.ru

Адрес: Россия, 350063, Краснодарский край, г. Краснодар, ул. Красина, д. 4.

Саенко Игорь Борисович – доктор технических наук, профессор. Ведущий научный сотрудник лаборатории проблем компьютерной безопасности. Санкт-Петербургский институт информатики и автоматизации Российской академии наук (СПИИРАН). Область научных интересов: автоматизированные информационные системы, информационная безопасность, обработка и передача данных по каналам связи, теория моделирования и математическая статистика, теория информации. E-mail: ibsaen@comsec.spb.ru

Адрес: Россия,199178, г. Санкт-Петербург, 14-я линия В.О., д. 39.

Synergistic approach to the management of sustainable functioning of the special purpose automatic systems

R. I. Zakharchenko, I. D. Korolev, I. B. Saenko

Annotation. The integration of diverse information systems of the state information system (GIS), including automated special-purpose systems of the Federal executive authorities (hereinafter referred to as the AS PS), through the public information and telecommunication networks (PITN) led to the availability of the AS PS through cyberspace. The functioning of the AS PS under conditions of targeted information and technical influences (ITI), especially the AS PS as a control object, as well as the uncertainty of knowledge about the environment and factors, goals and dynamics of their changes, led to the need to take into account the methodology and technologies to ensure the sustainability of the functioning of the sets factors previously did not occur. **The aim of this paper** is to develop a synergistic approach to managing the processes of ensuring the sustainability of the operation of an AS PS under conditions of cybernetic confrontation, as well as methods for its practical implementation. **The result and its novelty**. The article discusses a synergistic approach to building an adaptive decision support system (DSS) of the AS PS operating in ITI conditions in cyberspace. The proposed approach is based on a combination of multi-criteria utility methods in accordance with the criteria of optimality inherent in decision-making procedures, taking into account the current objective function and under given conditions. **The practical significance** of the presented approach is that it can be used in promising DSS to increase the adequacy of the management of the stability of the functioning of the AS PS, as well as the rationale for new forms and ways of conducting cyber warfare.

Key words: *cyberspace, informational technical influence (ITI), controlling of stability, synergistic approach, decision support system (DSS).*

Information about the Author

Roman Ivanovich Zakharchenko – Ph.D. Doctoral Candidate. Krasnodar Higher Military School named after army General S.M. Schtemenko. Research interests: management of complex information systems for special purposes, modeling the automation of special purpose control systems in the conditions of Cybernetics confrontation. E–mail: romanzakharchenko@yandex.ru

Igor' Dmitrievich Korolev – Ph.D, Full professor. Krasnodar Higher Military School named after army General S.M. Schtemenko. Research interests: management of complex information systems for special purposes, modeling the automation of special purpose control systems in the conditions of Cybernetics confrontation. E-mail: pi_korolev@mail.ru

Address: Russia, 350063, Krasnodar, Krasina, 4.

Igor Borisovich Saenko – Dr.Sci., Professor. Leading research scientist of Laboratory of Computer Security Problems. SPIIRAS. Research interests: automated information systems, information security, processing and transfer of data on data links, theory of modeling and mathematical statistics, information theory. E-mail: ibsaen@comsec.spb.ru

Address: Russia, 199178, St. Petersburg, SPIIRAS, 14-th line, 39.