АВТОМАТИЗАЦИЯ И УПРАВЛЕНИЕ ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ И ПРОИЗВОДСТВАМИ

DOI: 10.21821/2309-5180-2023-15-2-315-326

APPROACHES TO THE INTELLECTUALIZATION OF INFORMATION AND TELECOMMUNICATION NETWORKS SECURITY CONTROL IN TRANSPORT

Yu. I. Starodubtsev[1], Yu. K. Khudainazarov[2], T. P. Knysh[2]

[1] — Military Telecommunications Academy, St. Petersburg, Russian Federation
[2] — Admiral Makarov State University of Maritime and Inland Shipping, St. Petersburg, Russian Federation

The specifics of modern information and telecommunication networks in transport, as an object of information security control, are investigated. The main trends in the development of information and telecommunication network protection technologies (TNPT) have been identified. The presence of the interrelation of the main integrative properties: readiness, mobility, throughput, stealth, accessibility, manageability, which is a consequence of the convergence of information transmission and processing technologies, is noted. A new integrative property of ITCS has become the presence and characteristics of distributed system memory, which allows storing transmitted messages for a certain time. An important feature of modern TNPT is the presence of artificial intelligence, which is formed on the basis of information and algorithmic support of modern TNPT, providing flexibility of the system behavior. These trends indicate the transformation of TNPT into a supersystem, the management tasks of which are insufficiently investigated at present. The purpose of this work is to study new approaches to ensuring the safety management of modern TNPT critical infrastructure, which includes modern systems of sea and river transport, taking into account their features. The object of the study is the information security control system of modern TNPT. The subject of the study is the scientific and methodological support of the TNPT critical infrastructure control. The research objectives are to analyze existing and develop new conceptual frameworks, as well as approaches to improving the TNPT information security control system based on intellectualization methods. The analysis of the existing methodology for managing complex organizational and technical systems and information security control technologies is carried out. The concept of TNPT information security control is formalized schematically. The analysis of the existing approach to the organization of the TNPT information security control process is carried out. The tasks of control intellectualization are defined. The problem of ensuring the efficiency and reliability of the TNPT control is formulated. The main scientific tasks of the development of the TNPT information security control methodology are defined.

Keywords: information and telecommunication network, management concept, information security control, intellectualization, graphodynamics, multi-agent network, control system model.

For citation:
Starodubtsev, Yuri I., Yuri K. Khudainazarov, and Tatiana P. Knysh. "Approaches to the intellectualization of information and telecommunication networks security control in transport." *Vestnik Gosudarstvennogo universiteta morskogo i rechnogo flota imeni admirala S. O. Makarova* 15.2 (2023): 315–326. DOI: 10.21821/2309-5180-2023-15-2-315-326.

УДК: 654

ПОДХОДЫ К ИНТЕЛЛЕКТУАЛИЗАЦИИ КОНТРОЛЯ БЕЗОПАСНОСТИ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ НА ТРАНСПОРТЕ

Ю. И. Стародубцев[1], Ю. К. Худайназаров[2], Т. П. Кныш[2]

[1] — Военная академия связи имени маршала Советского Союза С. М. Будённого, Санкт-Петербург, Российская Федерация
[2] — ФГБОУ ВО «ГУМРФ имени адмирала С. О. Макарова», Санкт-Петербург, Российская Федерация

Исследована специфика современных информационно-телекоммуникационных сетей на транспорте как объекта контроля информационной безопасности. Определены основные тенденции развития технологий защиты информационно-телекоммуникационных сетей. Отмечается наличие взаимосвязи основных интегративных свойств: готовности, мобильности, пропускной способности, скрытности, доступности, управляемости, являющееся следствием конвергенции технологий передачи и обработки информации. Рассмотрено новое интегративное свойство информационно-телекоммуникационных сетей, такое как наличие характеристик распределенной системной памяти, позволяющей в течение определенного периода времени сохранять передаваемые сообщения. Важной особенностью современных информационно-телекоммуникационных сетей является наличие искусственного интеллекта, формируемого на основе их информационно-алгоритмического обеспечения, определяющего гибкость поведения системы. Указанные тенденции свидетельствуют о превращении в суперсистему, задачи управления которой недостаточно исследованы в настоящее время. Целью данной работы является исследование новых подходов к обеспечению управления безопасностью современных информационно-телекоммуникационных сетей критической инфраструктуры, к которой относятся современные системы морского и речного транспорта с учетом их особенностей. Объектом исследования служит система контроля информационной безопасности современных информационно-телекоммуникационных сетей. Предметом исследования является научно-методическое обеспечение контроля критической инфраструктуры. Задачи исследования заключаются в анализе существующих и разработке новых концептуальных основ, а также подходов к совершенствованию системы контроля информационной безопасности информационно-телекоммуникационных сетей на основе методов интеллектуализации. Выполнен анализ существующей методологии управления сложными организационно-техническими системами и технологий контроля информационной безопасности. Формализована схематично концепция контроля информационной безопасности информационно-телекоммуникационных сетей. Выполнен анализ существующего подхода к организации процесса контроля информационной безопасности информационно-телекоммуникационных сетей. Определены задачи интеллектуализации контроля. Сформулирована проблема обеспечения оперативности и достоверности контроля информационной безопасности информационно-телекоммуникационных сетей. Определены основные научные задачи развития методологии контроля информационной безопасности информационно-телекоммуникационных сетей.

Ключевые слова: информационно-телекоммуникационная сеть, концепция управления, контроль информационной безопасности, интеллектуализация, графодинамика, мультиагентная сеть, модель системы контроля.

Для цитирования:
Стародубцев Ю. И. Подходы к интеллектуализации контроля безопасности информационно-телекоммуникационных сетей на транспорте / Ю. И. Стародубцев, Ю. К. Худайназаров, Т. П. Кныш // Вестник Государственного университета морского и речного флота имени адмирала С. О. Макарова. — 2023. — Т. 15. — № 2. — С. 315–326. DOI: 10.21821/2309-5180-2023-15-2-315-326.

Введение (Introduction)

Современные информационно-телекоммуникационные сети (ИТКС) относятся к сложным динамическим социотехническим системам, генерирующим открытое множество информационных услуг, составной незначительной частью которых являются традиционные услуги связи. Принципиальные отличия ИТКС от системы связи заключаются в следующем:

– ИТКС создаются и развиваются в интересах многих систем управления работой флота;

– преобладающим является *способ коммутации пакетов*, что позволяет формировать виртуальные мультисервисные сети с высокой динамикой изменения структурных параметров;

– организационно-технические границы ИТКС *вариативны* в зависимости от количества, территориального размаха, количества и типа востребованных информационных услуг, что затрудняет выделение границ объекта контроля и усугубляет задачу определения оптимальных точек подключения средств контроля;

– контроль только состояния элементов ИТКС на технологическом уровне является недостаточным для управления качеством реализуемых процессов;

– подсистема контроля должна обеспечить потребности многих систем управления генерацией информационных услуг;

– существует устойчивая тенденция повышения информативности параметров трафика при сохранении и даже снижении информативности параметров технических средств;

– для большинства существующих ИТКС на организационном уровне затруднена или исключена возможность размещения средств контроля непосредственно на контролируемом объекте, так как элементы принадлежат различным собственникам, подвижны и пространственно распределены, поэтому необходимо совершенствование методов и технологий сетевого контроля;

– с учетом непрерывного совершенствования средств и способов защиты информационных ресурсов существенно затрудняется контроль ряда параметров, что вызывает необходимость разработки средств и способов защиты во взаимосвязи с процессом разработки методов и средств контроля.

Специфика современных ИТКС управления транспортом заключается в наличии тесной взаимной зависимости их основных интегративных свойств: готовности, мобильности, пропускной способности, скрытности, доступности, управляемости. Усиление взаимозависимости основных свойств является следствием конвергенции технологий. Кроме того, новым интегративным свойством ИТКС является наличие и характеристики распределенной системной памяти, позволяющей в течение определенного периода времени сохранять передаваемые сообщения, что существенно отражается на других свойствах сети.

Кроме того, особенность данных систем заключается в наличии агентов естественного и искусственного интеллекта, совокупность которых при определенных условиях образует суперсистему, поведение которой не может быть в полной мере формализовано в рамках классической теории управления. Трудности формализации связаны с высокой степенью неопределенности инфраструктуры и влиянием человеческого фактора в процессе функционирования суперсистемы. Суперсистема отличается виртуальностью функциональной структуры, т. е. существованием элементов (подсистем), которые обладают памятью, могут обмениваться между собой информацией, в определенной степени взаимозаменяемы и в разные моменты времени могут принадлежать к системам, имеющим различный функционал. При этом возможны *конфликты управления системами* (информационные конфликты, конфликты по задачам, ресурсам и времени).

Информационно-алгоритмическое обеспечение современной ИТКС, являясь многоуровневым, включает *фундаментальную* (статическую) и *адаптационную* (динамическую) часть, замена которой обеспечивает новую специализацию элементов. Примером являются технологии *Soft Definition Network (SDN)*, *Network Function Virtualization (NFV)*, *Soft Definition Radio (SDR).* В связи с этим ИТКС в целом обладает памятью и гибкостью поведения, для устойчивого функционирования которой должно выполняться следующее условие: *скорость адаптации элементов к новым функциональным задачам должна быть выше скорости изменения внешних воздействующих факторов.* В связи с этим актуальной является тематика исследований существующих и разработка новых подходов к обеспечению качественной обратной связи в системе управления безопасностью современных ИТКС критической инфраструктуры, что и составляет *цель данной работы*.

Задачи исследования заключаются в анализе методологии контроля безопасности информации в ИТКС критической инфраструктуры, выявлении противоречий в практике и теории контроля безопасности ИТКС, определении новых требований к результатам контроля информационной безопасности ИТКС, формулировке проблемы интеллектуализации контроля ИБ ИТКС, а также разработке подходов к решению проблемы и построению интеллектуальной системы контроля информационной безопасности ИТКС, обеспечивающей выполнение заданных критериев по качеству управления ИБ ИТКС критической инфраструктуры.

Методы и материалы (Methods and Materials)

Существующая методология управления сложными системами предполагает определение необходимых условий для организации управления [1]: устойчивости в части предсказуемости поведения и полной функции управления системы. Устойчивость обусловлена существованием объективных причинно-следственных связей, а предсказуемость поведения основана на их субъективной интерпретации. Мера достаточности предсказуемости также определяется субъективно,

исходя из интерпретации задачи управления системой по полной функции, в том числе по функциям информационной безопасности (ИБ).

Полная функция управления (ПФУ), представляющая собой иерархически упорядоченную последовательность различных действий, может осуществляться только *интеллектуальной системой* [1]. ПФУ включает следующие этапы (рис. 1):

1-й этап — опознание управляемого объекта и факторов среды;

2-й этап — формирование модели объекта и факторов среды;

3-й этап — формирование вектора целей управления объектом в отношении факторов среды на основе решения задачи об устойчивости в смысле предсказуемости его поведения;

4-й этап — формирование концепции управления и частных целевых функций управления на основе решения задачи об устойчивости в смысле предсказуемости поведения объекта для обеспечения требуемого качества управления;

5-й этап — организация и реорганизация управляющих структур, несущих целевые функции управления;

6-й этап — контроль функционирования структур в процессе управления, координация взаимодействия разных структур;

7-й этап — ликвидация управляющих структур в случае необходимости или поддержание их в работоспособном состоянии до следующего использования.

Формирование концепций управления предполагает задание вектора параметров управляющих воздействий и значений параметров ошибки управления в виде разности значений параметров текущего состояния ИТКС и требуемых значений параметров состояния [1]. Однако подобные линейные функции оценки качества управления недостаточны для контроля сложной системы с интегративными свойствами. При наличии зависимости между показателями функционирования суперсистемы оценка качества управления определяется *приоритетами ее частных показателей функционирования, т. е. динамикой.* В зависимости от характера внешних связей суперсистемы со средой возможны задачи управления ИТКС как единым целым, так и ее отдельными фрагментами (элементами). Кроме того, в зависимости от продолжительности воздействия внешних факторов возможно непрерывное управляющее воздействие, регулярно повторяющееся или статистически упорядоченное эпизодическое. Поэтому соответствующие управляющие структуры будут *постоянно действующими*, *циклически действующими* или *стохастическими*. В зависимости от характера взаимодействий в суперсистеме возможны прямые и обратные связи типа: «человек – человек», «человек – машина», «человек – система», «машина – машина», «система – система».

Контроль, являющийся обратной связью полной функции управления, выполняется дважды (рис. 1): на первом этапе — при опознавании объекта и факторов среды для обоснования структуры системы управления и на последнем этапе — при обеспечении функционирования управляющих структур для анализа и повышения качества взаимодействия разных структур. Организация контроля является самостоятельной задачей, которая решается на основе оптимизации экономических параметров системы при обязательном выполнении задач контроля требуемого качества. Для управления в отношении постоянных, периодических или случайных факторов необходима соответствующая система, которая должна обеспечивать требуемое качество обратной связи и может иметь, соответственно, устойчивую структуру или виртуальный характер.

Существующие в настоящее время технологии сбора и обработки данных контролируемых параметров и событий (*EDR, IRP, SIEM*), управления уязвимостями (*VM*) позволяют сформировать большие базы данных о состоянии ИТКС в близком к реальному масштабу времени. В то же время возникает *проблема унификации форматов представления и обработки больших данных* для обеспечения интегральной оценки состояния ИТКС и интеллектуальной поддержки решений (построения базы знаний) по управлению ИТКС [2].

Большинство существующих форматов представления данных в человеко-машинных системах не эргономичны, а протоколы взаимодействия машин и систем *проприеритарны*, поэтому не позволяют в полной мере обеспечивать взаимодействие одновременно по вертикали и горизонтали

и в связи с этим реализовать матричную схему управления (сетецентрическую) не представляется возможным. Таким образом, существуют технологические недостатки, не позволяющие решить задачи взаимодействия и контроля в современных ИТКС.

Рис. 1. Концепция управления сложными системами

К организации контроля относятся [3]:
– стратегия (концепция) контроля;
– схема обслуживания;
– органы контроля и их задачи;
– оборудование (средства) контроля;
– схема централизованной обработки результатов контроля;
– порядок проверки работоспособности, диагностики и восстановления средств контроля.

Концепция контроля — это система взглядов, идей, принципов, определяющих общую методологию контроля, основное содержание которой составляют ответы на вопросы ~~*что*~~, *где*, *когда*, *как* и *каким образом* контролировать соответствующую систему управления для обеспечения ее функционирования (рис. 2). Первой составляющей концепции является определение границ контролируемого объекта (процесса) и ограничений с учетом условий внешней среды (внешние воздействующие факторы, характеристики объемлющей системы, пространственные и информационные метрики, взаимосвязи), а также состава векторов контролируемых параметров объекта (процесса), внешних факторов и управляющих воздействий, которые определены *концепцией управления*.

Первая составляющая концепции является метрологической моделью контроля; формализуется в виде модели контролируемого объекта (процесса), каталога задач контроля и вектора контролируемых параметров.

Второй составляющей концепции контроля является определение соотношения функциональных циклов изменения и причинно-следственных взаимосвязей между событиями, характеристиками контролируемых процессов, объектов в пределах указанных ранее ограничений (определение степени устойчивости объекта (процесса) по предсказуемости при заданной концепции управления); формализуется в виде модели процесса контроля и критериев качества результатов контроля.

Третьей составляющей концепции контроля является обоснование структуры системы, выбора форм, методов и способов оценки соответствия состояния объекта (процесса), внешней среды (объемлющей системы), управляющих воздействий в соответствии с заданными критериями качества результатов контроля; формализуется в виде модели системы контроля, отвечающей установленным требованиям.

Рис. 2. Концепция контроля при управлении сложными социотехническими системами

Частные концепции контроля определяют методологию контроля для реализации каждой из задач управления свойствами объекта (процесса). Управление информационной безопасностью (ИБ) ИТКС осуществляется в соответствии с частной концепцией ИБ. В условиях преднамеренного информационно-технического воздействия (ИТВ) на ИТКС управления транспортом необходимо рассматривать взаимоотношения среды функционирования и ИТКС в форме *информационного конфликта*. Основной целевой функцией управления ИБ ИТКС на транспорте в условиях информационного конфликта является минимизация времени выявления уязвимости ИТКС, обнаружения деструктивного фактора и достижение требуемого качества управления ресурсами, выделяемыми для его нейтрализации в течение периода конфликтной ситуации. С позиций концепции информационного противоборства сущность информационного конфликта заключается в создании средствами ИТВ угроз нарушения безопасности информации в ИТКС и реагировании их на угрозы (рис. 3).

Рис. 3. Концепция управления информационной безопасностью

Для противодействия ИТВ в ИТКС на транспорте организуется система обеспечения информационной безопасности (СОИБ). Исход информационного конфликта в условиях ИТВ и ограниченных транспортно-вычислительных ресурсов системы защиты ИТКС управления транспортом в существенной степени зависит от качества управления ими. В процессе управления ИТКС для обоснования стратегий, форм, методов и способов целенаправленного поведения СОИБ при информационном конфликте необходимо выявить закономерности поведения систем ИТВ и СОИБ [4].

Результаты (Results)

Для реализации целевой функции контроля ИБ ИТКС необходима разработка соответствующей концепции, формализующей закономерные взаимосвязи процессов возникновения уязвимостей ИТКС, воздействия ИТВ и управления СОИБ ИТКС по критерию минимизации времени обнаружения и обработки инцидентов, а также обоснование критериев своевременности (оперативности) цикла управления функциями безопасности (рис. 4). Модель должна включать модель СОИБ как объекта контроля, модель угроз ИБ ИТКС и модель процесса (системы) контроля информационной безопасности ИТКС.

Рис. 4. Концепция контроля информационной безопасности ИТКС

Известные подходы оценки состояния ИТКС на основе вероятностных графов [5] основаны на предположении о марковских свойствах моделируемых процессов и достаточности статистических данных для перехода к вероятностным характеристикам событий. В связи с этим метод вероятностных графов ограничен статическими свойствами оцениваемого объекта, не позволяя в полной мере обеспечивать близкий к реальному масштабу времени контроль.

Статистика уязвимостей и инцидентов безопасности объектов ИТКС на транспорте показывает низкую эффективность существующих подходов к организации системы и применяемых методов контроля ИБ. Известные методы обработки больших данных в настоящее время являются недостаточно эффективными, что, в частности, обусловлено снижением содержательности обрабатываемых данных вследствие упрощения алгоритмов оценки частных и обобщенных показателей ИБ ИТКС и снижением критериев оценки ИБ для повышения оперативности контроля.

Традиционная схема контроля ИБ ИТКС в настоящее время (рис. 5) предполагает *централизованную обработку данных контроля*, которые передаются в центр управления безопасностью (*Security Operation Centre*) по основным информационным каналам в виде неприоритетного трафика.

Рис. 5. Традиционная схема процесса контроля ИБ ИТКС.

Необходимыми условиями обеспечения полноты, достоверности и своевременности контроля ИБ являются:

– энтропия (количество степеней свободы) системы контроля ИБ должна быть не меньше энтропии ИТКС;

– скорость (частота) изменения (адаптации) агентов контроля должна быть не меньше скорости изменения ИТКС.

Обсуждение (Discussion)

Гипотеза данного исследования заключается в том, что для обеспечения качественного управления ИБ интеллектуальной ИТКС необходимо развитие существующих подходов к контролю ИБ на основе *интеллектуализации соответствующей системы контроля ИБ* и увеличение за счет этого количества ее степеней свободы (гибкости). Гибкость в данном случае предполагает возможность обоснованного выбора критериев качества контроля ИБ ИТКС, а также самоорганизации системы контроля ИБ.

Интеллект, обеспечивающий управление суперсистемой, называется *сопряженным* и может быть внешним по отношению к суперсистеме, внутренним или порождаться самой суперсистемой [1]. Интеллектуализация на этапах полной функции управления обеспечивает опознавание воздействующих факторов и определение целевой функции управления, а также формулирование соответствующих частных концепций управления в отношении каждого из воздействующих факторов.

Интеллектуализация контроля безопасности информации в ИТКС предполагает решение *задачи самоорганизации системы* (выбора форм, методов и способов) для обеспечения заданного качества контроля в условиях высокой динамичности ИТКС, а также при поддержке решений по координации вычислительных и транспортных ресурсов ИТКС, выделяемых для обеспечения контроля ИБ: биллинговой системы, системы управления качеством обслуживания QoS, ресурсов гибких коммутаторов (контроллеров), COPM, DLP [6]. Известные системы управления ИТКС используют *модели ситуационного управления*, в которых интеллектуализация контроля обеспечивается искусственными нейронными сетями (ИНС).

Качественную шкалу возрастания потенциала решения задач управления с помощью интеллектуализации можно представить следующим образом: программное управление; управление с обратной связью; ситуационное управление; адаптивное управление; интеллектное управление (без целеполагания); интеллектуальное управление (с целеполаганием) [7]. Концепция ИНС предполагает модель *базового процессорного элемента* (рис. 6) и различные варианты структуры многослойных сетей, адаптируемых для решения конкретной задачи с помощью *методов машинного обучения* [8]. Требования к объему обучающей выборки и времени обучения для адаптации к изменяющимся условиям функционирования объекта контроля являются одним из недостатков данной технологии [9].

Существующие подходы и методы машинного обучения искусственных нейронных сетей ограничены предположением о репрезентативности обучающей выборки событий, однако в современных условиях высокой динамики угроз ИБ данное предположение делает необходимыми обоснование и контроль адекватности модели обучающей выборки. Широкое применение находит *агентно-ориентированный подход* к построению распределенных систем контроля состояния ИТКС.

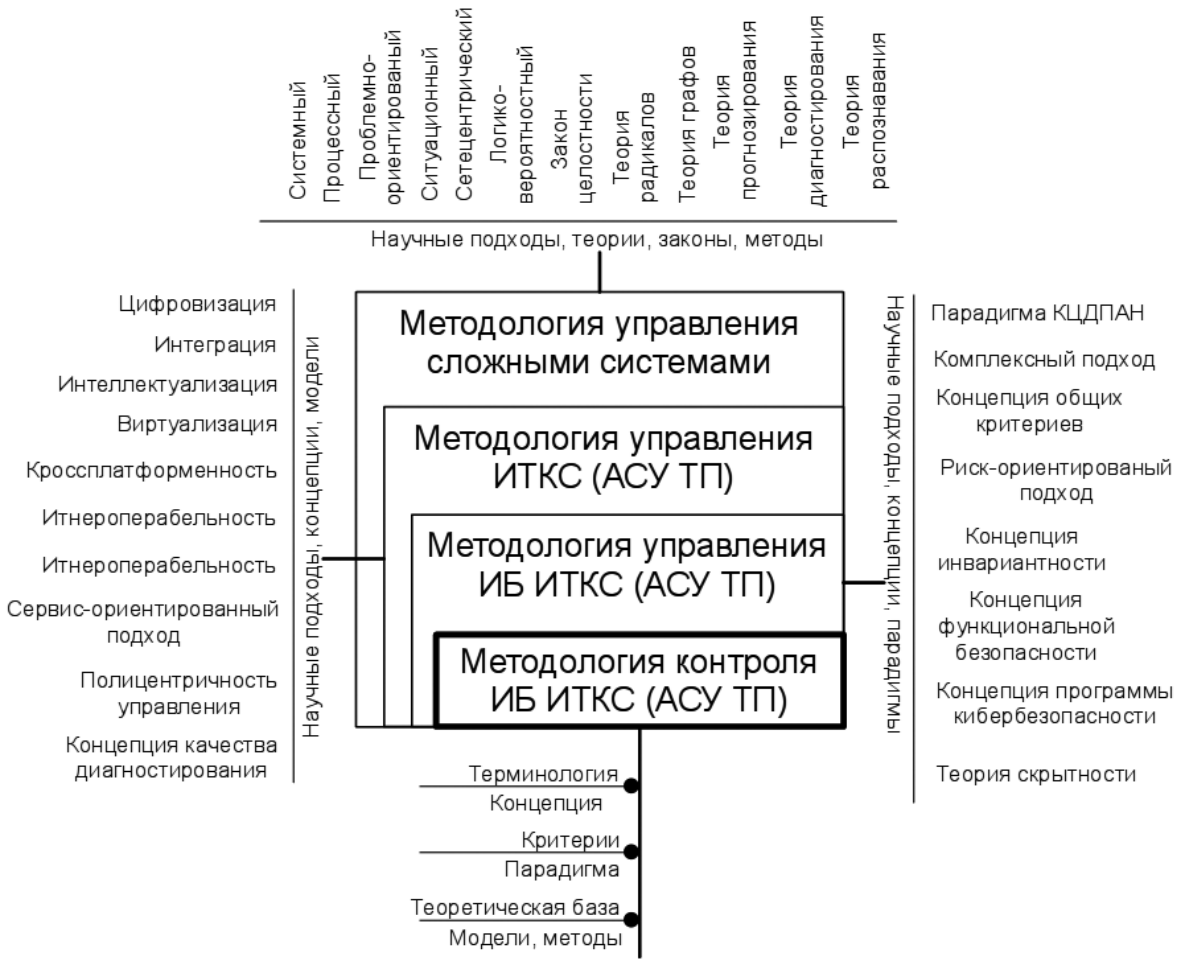

Рис. 6. Обобщенная архитектура методологии управления ИБ ИТКС

Задача координации ресурсов, разделяемых между процессами при управлении мультиагентной сетью контроля ИБ ИТКС, является одной из проблем организации распределенных и параллельных вычислений в условиях многопротокольности взаимодействия и многоформатности данных. Кроме того, современные системы мониторинга ИТКС генерируют бесконечный поток событий безопасности, которые для обеспечения полноты охвата контролем и обеспечения режима реального времени настроены на фиксацию изменений параметров каждого из элементов системы без детализации его состояния. По этой причине возникает переизбыток сообщений и недостаток их контекста, что усложняет для ЛПР задачу идентификации состояния безопасности и требует дополнительных проверок, следовательно, снижается оперативность реагирования на инциденты безопасности. Таким образом, возникает задача обработки в режиме, близком к реальному времени, большого потока сообщений о событиях безопасности без потери их содержательности. Для решения этой задачи целесообразно исследование *феномена афферентного синтеза* применительно к задачам оценки ИБ ИТКС [10] и дополнение существующей нейросетевой модели системы контроля моделью иерархической параллельной обработки данных контроля.

Графодинамическое представление процесса сбора и обработки данных о контролируемых параметрах ИБ позволяет организовать параллельную обработку больших данных контроля с учетом малоинформативных контролируемых параметров в масштабе времени, близком к реальному. Известные подходы исчисления древовидных структур позволяют существенно снизить трудоемкость программирования в ресурсах глобальных ИТКС путем построения *унифицированных функций отображения* [11]. Однако в настоящее время прикладные аспекты теории графодинамики и исчисления древовидных структур, применимые для решения задач организации контроля

ИБ ИТКС, недостаточно исследованы. Следовательно, требуется разработка методов и моделей, для формализации процесса контроля ИБ и возможности комбинирования постоянных, периодически формируемых и стохастически самоорганизующихся (виртуальных) структур системы контроля ИБ с учетом важности (приоритетности) контролируемых параметров ИБ ИТКС, а также обеспечивающих унификацию протоколов взаимодействия и форматов представления данных.

В связи с динамичностью и неопределенностью границ между виртуальными системами, а также их структуры, неопределенностью описания человеческого фактора возникает необходимость использования нечеткой логики при моделировании процессов в ИТКС. Существующие модели нечетких семантических сетей недостаточно исследованы в аспекте формализации критериев оценки ИБ ИТКС.

Таким образом, интенсивность нарастания энтропии современной ИТКС при ее функционировании такова, что контролировать состояние и управлять ИБ ИТКС в реальном масштабе времени в рамках существующей концепции и методологии невозможно вследствие невыполнения условия достаточной предсказуемости ее поведения. Приведенные недостатки в практике, а также в теории контроля ИБ ИТКС свидетельствуют о существовании проблемы, заключающейся в том, что известные модели и методы управления ИБ ИТКС (см. рис. 6), базирующиеся на существующих концепциях и научных подходах, не позволяют разрешить противоречия в теории контроля ИБ ИТКС [12].

Заключение (Conclusion)

Проведенный анализ подходов и методов контроля состояния ИТКС позволяет выдвинуть гипотезу о том, что повышение качества управления ее ИБ возможно за счет синтеза интеллектуальной системы контроля ИБ ИТКС на основе теории функциональных систем и формализации процесса афферентного синтеза. Сокращение цикла контроля ИБ возможно на основе нового подхода к обеспечению самоорганизации системы контроля ИБ по заданным критериям качества результатов контроля путем автоматической генерации заданий (профилей) контроля и самосинхронизации мультиагентной сети контроля. Повышение достоверности результатов контроля возможно путем разработки метода унификации форматов представления данных и протоколов обмена данными в мультиагентной сети контроля на основе моделей графодинамики и древовидных структур. Каждый уровень декомпозиции ИТКС (инфраструктуры, услуг, приложений) может контролироваться соответствующим слоем синтезированной сети агентов, что позволяет создать универсальную технологическую платформу. В связи с этим в рамках развития методологии контроля ИБ ИТКС актуальным является решение следующих научных задач [13]:

1. Разработка графодинамической модели системы контроля ИБ ИТКС с сетецентрическим управлением мультиагентной сетью агентов контроля ИБ.

2. Разработка метода логического вывода иерархического дерева задач контроля (профилей контроля) для каждого типа контролируемых объектов с учетом данных о текущем состоянии ИТКС, внешних условий и доступности ресурсов системы контроля ИБ на основе исчисления древовидных структур.

3. Разработка метода обработки данных контроля и свертки частных показателей ИБ в виде нечеткой семантической сети.

СПИСОК ЛИТЕРАТУРЫ

1. Достаточно общая теория управления (ДОТУ). — Вторая редакция 2003–2004 гг. — М.: НОУ «Академия управления», 2011. — 416 с.

2. *Лепешкин О. М.* Концепция интеллектуализации контроля безопасности связи в информационно-телекоммуникационной сети специального назначения / О. М. Лепешкин, Ю. К. Худайназаров // Состояние и перспективы развития современной науки по направлению «Информационная безопасность»: сб. статей III Всеросс. науч.-техн. конф. — Анапа: Военный инновационный технополис «ЭРА», 2021. — С. 697–709.

3. *Евланов Л. Г.* Контроль динамических систем / Л. Г. Евланов. — 2-е изд., перераб. доп. — М.: Наука (Главная редакция физико-математической литературы), 1979. — 432 с.

4. *Жидко Е. А.* Модель подсистемы безопасности и защиты информации системы связи и управления критически важного объекта / Е. А. Жидко, С. Н. Разиньков // Системы управления, связи и безопасности. — 2018. — № 1. — С. 122–135.

5. *Аллакин В. В.* Идентификация состояния узлов информационно-телекоммуникационных сетей общего пользования подсистемой мониторинга информационной безопасности / В. В. Аллакин, Н. П. Будко // Техника средств связи. — 2020. — № 3 (151). — С. 58–65.

6. *Шуравин А. С.* Анализ применимости DLP-систем для мониторинга безопасности распределенных сетей связи специального назначения / А. С. Шуравин // Актуальные проблемы защиты и безопасности / Труды XXIII Всеросс. науч.-практ. конф. РАРАН. — М.: РАРАН, 2020. — Т. 1. — С. 278–281.

7. *Чинакал В. О.* Интеллектуальные системы и технологии: учеб. пособие / В. О. Чинакал. — М.: РУДН, 2008. — 303 с.

8. *Терехов В. А.* Нейросетевые системы управления / В. А. Терехов, Д. В. Ефимов, И. Ю. Тюкин, В. Н. Антонов. — СПб: Изд-во СПб. ун-та, 1999. — 265 с.

9. *Худайназаров Ю. К.* Интеллектуализация разрешения неопределенности информации при синтезе и анализе системы обеспечения безопасности критически важного объекта / Ю. К. Худайназаров, П. А. Новиков, А. С. Шуравин, К. Н. Киселев // Нейрокомпьютеры и их применение / XVII Всеросс. науч. конф.: тез. докл. — М.: МГППУ, 2019. — С. 62–64.

10. *Анохин П. К.* Биология и нейрофизиология условного рефлекса / П. К. Анохин. — М.: Медицина, 1968. — 546 с.

11. *Затуливетер Ю. С.* Графодинамические системы с сетецентрическим управлением в математически однородном поле компьютерной информации / Ю. С. Затуливетер, Е. А. Фищенко // Управление большими системами: сб. тр. — 2010. — № 30–1. — С. 567–604.

12. *Лепешкин О. М.* Проблема контроля и мониторинга информационной безопасности информационно — телекоммуникационной сети специального назначения / О. М. Лепешкин, Ю. К. Худайназаров // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. — 2020. — № 7–8 (145–146). — С. 49–55.

13. *Худайназаров Ю. К.* Задачи системы интеллектуального мониторинга информационной безопасности инфотелекоммуникационной сети / Ю. К. Худайназаров, А. С. Пермяков, Е. О. Лепешкин // Нейрокомпьютеры и их применение / XVIII Всеросс. науч. конф.: тез. докл. — М.: МГППУ, 2020. — С. 198–200.

REFERENCES

1. *Dostatochno obshchaya teoriya upravleniya. (Vtoraya redaktsiya 2003–2004 gg.).* M.: NOU «Akademiya upravleniya», 2011.

2. Lepeshkin, O. M., and Yu. K. Khudainazarov. “Kontseptsiya intellektualizatsii kontrolya bezopasnosti svyazi v informatsionno-telekommunikatsionnoi seti spetsial’nogo naznacheniya.” *Sostoyanie i perspektivy razvitiya sovremennoi nauki po napravleniyu «Informatsionnaya bezopasnost’». Sbornik statei III Vserossiiskoi nauchno-tekhnicheskoi konferentsii*. Anapa: Federal’noe gosudarstvennoe avtonomnoe uchrezhdenie “Voennyi innovatsionnyi tekhnopolis “ERA”, 2021. 697–709.

3. Evlanov, L. G. *Kontrol’ dinamicheskikh sistem*. 2nd ed. M.: Nauka. Glavnaya redaktsiya fiziko-matematicheskoi literatury, 1979.

4. Zhidko, Elerna Aleksandrovna, and Sergey Nikolaevich Razinkov. “Model of security and information protection subsystem of a communication and control system of a critical object.” *Systems of Control, Communication and Security* 1 (2018): 122–135.

5. Allakin, V. V., and N. P. Budko “Identification of the state of nodes of public information and telecommunications networks by the information security monitoring subsystem.” *Means of communication equipment* 3(151) (2020): 58–65.

6. Shuravin, A. S. “Analiz primenimosti DLP-sistem dlya monitoringa bezopasnosti raspredelennykh setei svyazi spetsial’nogo naznacheniya.” *Aktual’nye problemy zashchity i bezopasnosti. Trudy XXIII Vserossiiskoi nauchno-prakticheskoi konferentsii RARAN.* Vol. 1. M.: Rossiiskaya akademiya raketnykh i artilleriiskikh nauk, 2020. 278–281.

7. Chinakal, V. O. *Intellektual’nye sistemy i tekhnologii*. M.: RUDN, 2008.

8. Terekhov, V. A., D. V. Efimov, I. Yu. Tyukin, and V. N. Antonov. *Neirosetevye sistemy upravleniya*. SPb: Izd. S-Peterburgskogo universiteta, 1999.

9. Khudainazarov, Yu. K., P. A. Novikov, A. S. Shuravin, and K. N. Kiselev. "Intellektualizatsiya razresheniya neopredelennosti informatsii pri sinteze i analize sistemy obespecheniya bezopasnosti kriticheski vazhnogo ob"ekta." *Neirokomp'yutery i ikh primenenie. XVII Vserossiiskaya nauchnaya konferentsiya. Tezisy dokladov.* M.: Moskovskii gosudarstvennyi psikhologo-pedagogicheskii universitet, 2019. 62–64.

10. Anokhin, P. K. *Biologiya i neirofiziologiya uslovnogo refleksa*. M.: Meditsina, 1968.

11. Zatuliveter, Yurii Semenovich, and Elena Alekseevna Fischenko. "Graph-dynamics systems with network-centric control in mathematically uniform field of computer information." *Large-Scale Systems Control* 30–1 (2010): 567–604.

12. Lepechkin, Oleg Mihailovich, and Yurj Kahramonovich Khudajnazarov. "The problem of the checking and monitoring to information safety information — telecommunication network of the special purpose." *Defense Engineering Problems. Series 16. Technical means of combating terrorism* 7–8(145–146) (2020): 49–55.

13. Khudainazarov, Yu. K., A. S. Permyakov, and E. O. Lepeshkin. "Zadachi sistemy intellektual'nogo monitoringa informatsionnoi bezopasnosti infotelekommunikatsionnoi seti." *Neirokomp'yutery i ikh primenenie. XVIII Vserossiiskaya nauchnaya konferentsiya. Tezisy dokladov.* M.: Moskovskii gosudarstvennyi psikhologo-pedagogicheskii universitet, 2020. 198–200.

ИНФОРМАЦИЯ ОБ АВТОРАХ

Стародубцев Юрий Иванович —
доктор военных наук, профессор
Военная академия связи имени маршала Советского Союза С. М. Будённого
193064, Российская Федерация, Санкт-Петербург, Тихорецкий проспект, 3
e-mail: *starodub@mail.ru*

Худайназаров Юрий Кахрамонович —
кандидат технических наук
ФГБОУ ВО «ГУМРФ имени адмирала С. О. Макарова»
198035, Российская Федерация, Санкт-Петербург, ул. Двинская, 5/7
e-mail: *yu-78@ya.ru*

Кныш Татьяна Петровна —
кандидат физико-математических наук, доцент
ФГБОУ ВО «ГУМРФ имени адмирала С. О. Макарова»
198035, Российская Федерация, Санкт-Петербург, ул. Двинская, 5/7
e-mail: *knyshtp@gumrf.ru*

INFORMATION ABOUT THE AUTHORS

Starodubtsev, Yuri I. —
Dr. of Military Sciences, professor
Military Telecommunications Academy
3 Tikhoretsky Ave.,
St. Petersburg, 193064,
Russian Federation
e-mail: *starodub@mail.ru*

Khudainazarov, Yuri K. —
PhD
Admiral Makarov State University of Maritime and Inland Shipping
5/7 Dvinskaya Str., St. Petersburg, 198035,
Russian Federation
e-mail: *yu-78@ya.ru*

Knysh, Tatiana P. —
PhD, associate professor
Admiral Makarov State University of Maritime and Inland Shipping
5/7 Dvinskaya Str., St. Petersburg, 198035,
Russian Federation
e-mail: *knyshtp@gumrf.ru*

Статья поступила в редакцию 6 февраля 2023 г.
Received: February 6, 2023.