СИСТЕМНЫЙ АНАЛИЗ И УПРАВЛЕНИЕ
SYSTEM ANALYSIS AND PROCESSING OF KNOWLEDGE

УДК 006.88, 007.51
DOI

КОНЦЕПТУАЛЬНЫЕ ОСНОВЫ ОБЕСПЕЧЕНИЯ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ

CONCEPTUAL BASES OF MAINTENANCE OF COMPLEX SAFETY ON CRITICAL OBJECTS

А.И. Офицеров[1], О.О. Басов[2], С.С. Бачурин[1]
A.I. Ofitserov[1], O.O. Basov[2], S.S. Batchurin[1]

[1)] Федеральное государственное казенное военное образовательное учреждение высшего образования «Академия Федеральной службы охраны Российской Федерации», Россия, 302015, Орел, ул. Приборостроительная, д. 35
[2)] Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики», Россия, 197101, Санкт-Петербург, Кронверкский пр., д. 49

[1)] The Federal state government military educational institution of higher education «The Academy of the Federal Guard Service of the Russian Federation», 35 Priborostroitelnaya St, Orel, 302015, Russia
[2)] Saint Petersburg National Research University of Information Technologies, Mechanics and Optics, 49 Kronverkskiy Ave, Petersburg, 197101, Russia

E-mail: oficerow@mail.ru, oobasov@mail.ru

Аннотация
Данная статья посвящена рассмотрению проблемы обеспечения комплексной безопасности критически важных объектов, обуславливающей объективную актуальность создания концептуальной платформы, на основе которой возможна реализация многоуровневых автоматизированных систем обеспечения комплексной безопасности критически важных объектов. В работе проведен проблемно-классификационный анализ существующих методов и способов обеспечения безопасности критически важных объектов и построения систем обеспечения комплексной безопасности. Установлено, что наиболее эффективным решением обозначенной проблемы является реализация метода синтеза структуры системы при заданных алгоритмах и принципах функционирования отдельных ее подсистем. Представленный в работе агрегативно-декомпозиционный подход к построению систем обеспечения комплексной безопасности критически важных объектов позволяет, в зависимости от уровня детализации реализуемых системой целей, выполняемых функций и задач, поставить и решить ряд типовых задач синтеза ее структуры.

Abstract
The given article is devoted to the consideration of a problem of maintenance of complex safety of critical objects causing an objective urgency of creation of a conceptual platform on which basis realization of the multilevel automated systems of maintenance of complex safety on critical objects is possible. In work the problem-classification analysis of existing methods and ways of safety of crucial objects and construction of systems of maintenance of complex safety is carried out. It is established that the most effective decision of the designated problem is the realization of a method of synthesis of the structure of the system at the set algorithms and principles of functioning of its separate subsystems. Presented in the work the aggregative-decomposition approach to construction of the systems of maintenance of complex safety of critical objects allows, depending

on the level of detailed elaboration of the purposes realized by the system, carried out functions and problems, to put and solve a number of typical problems of its structure's synthesis.

Ключевые слова: критически важный объект, комплексная безопасность, агрегативно-декомпозиционный подход, синтез системы, альтернативно-графовая формализация.
Keywords: critical objects, complex safety, aggregative-decomposition approach, system synthesis, alternatively-graph formalization.

Введение

В настоящее время безопасность критически важных объектов (КВО) от реальных и потенциальных угроз различного характера обеспечивается применением совокупности правовых, охранных, режимных, оперативно-розыскных, материально-технических, информационных и иных мер с использованием технических комплексов и технологических процессов, основа которых была заложена в 60-е – 80-е годы прошлого столетия. Реализация таких процессов связана с широким применением ручного труда, а приход новых образцов технических средств не внес в них существенных изменений, не позволил освободиться от монотонных и трудоемких критически важных технологических процедур, в то же время значительно усложнил их, не дав ожидаемого положительного эффекта.

Кроме того, совокупность принимаемых мер по обеспечению безопасности КВО в значительной степени обусловлена разрозненностью структуры сил, разнонаправленностью решаемых ими задач, отсутствием единого замысла и центра управления. Как следствие, при взаимодействии отмечаются конфликты интересов, дублирование или отсутствие части необходимых мер при решении конкретных задач обеспечения безопасности критически важных объектов, что в свою очередь повышает финансовые затраты для их решения, снижает производительность труда и эффективность финансирования, что особенно важно в условиях дефицита бюджетных средств.

Участившиеся в последнее время акты международных террористических организаций и активизация деятельности иностранных спецслужб по реализации гибридных угроз на территории Российской Федерации и в сопредельных государствах значительно актуализируют проблему защиты КВО на всех уровнях их иерархической структуры в связи с критическими и зачастую глобальными последствиями нарушения безопасности функционирования данных объектов. Существенно изменившиеся за последнее время источники потенциальных угроз безопасности КВО, методики их осуществления обуславливают актуальность разработки новых эффективных способов оценки рисков, а также комплекса мер по обнаружению и нейтрализации угроз безопасности.

Таким образом, на данный момент возникла объективная необходимость создания концептуальной платформы, на основе которой возможна реализация многоуровневых автоматизированных систем обеспечения комплексной безопасности (СОКБ) КВО. Данная платформа позволит повысить уровень защищенности КВО, создать эффективную структуру его безопасности, основанную на системности, актуальности существующим и перспективным угрозам, снизить трудозатраты и повысить экономическую эффективность. Все это требует разработки новых элементов теории построения СОКБ КВО.

1. Проблемно-классификационный анализ существующих методов и способов обеспечения комплексной безопасности критически важных объектов

Совершенствование принципов построения современных систем безопасности КВО неразрывно связано со сложными процессами их автоматизации и интеграции, которые также касаются и всех остальных систем, например, жизнеобеспечения и управления функционированием данных объектов. Обоснованным результатом такой интеграции является создание СОКБ, позволяющих автоматизировать управление всеми системами

КВО, а также реализовать комплекс мер, направленных на выявление наиболее опасных угроз и критических ситуаций, оценку вероятного ущерба от этих угроз и ситуаций, и обеспечивающих таким образом непрерывное и стабильное функционирование объекта. Обеспечение комплексной безопасности КВО представляет собой сложный и многогранный процесс реализации совокупности правовых, режимных, охранных, оперативно-розыскных, материально-технических, информационных и иных мероприятий, осуществляемый для достижения максимальной защищенности объектов от реальных и потенциальных угроз социального, техногенного и природного характера (рис. 1).

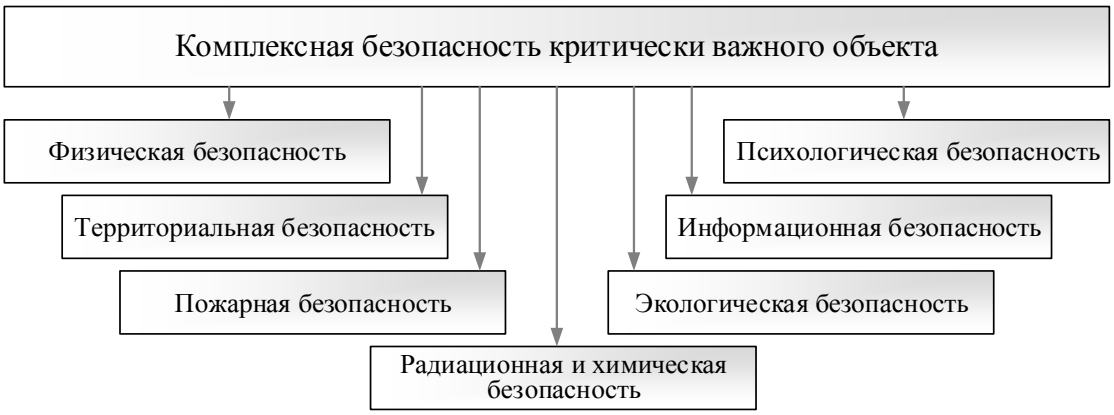

Рис. 1. Составляющие комплексной безопасности критически важного объекта
Fig. 1. Components of complex safety of a critical object

Современные исследования в области построения оптимальных сложных технических систем (в том числе СОКБ) многих зарубежных и отечественных ученых крайне многогранны, но все же еще далеки от совершенства. Основные результаты данных исследований, изложенные в различных научных трудах, посвящены в основном либо проблемам разработки и оценки систем физической защиты (СФЗ) и отдельных ее подсистем, либо вопросам обеспечения информационной безопасности без учета их взаимодействия с другими системами безопасности, в совокупности образующими СОКБ. Так, теоретические подходы к вопросам разработки, анализа и оценки СФЗ нашли отражение в работе [Гарсия, 2002], в которой подробно описана методика оценки уязвимости объектов, рассмотрены вопросы оценки эффективности СФЗ, разработки моделей нарушителя и угроз.

Из отечественных работ, посвященных вопросам анализа и синтеза СФЗ, наиболее фундаментальной является диссертация [Боровский, 2015], в которой исследован комплексный подход к интеграции процессов интеллектуальной поддержки принятия проектных решений в задачах разработки и оценки СФЗ КВО на основе системного анализа и экспертных знаний, а также разработаны оптимизационные модели, алгоритмы и методы оценки защищенности КВО в условиях неопределенности.

В монографии [Бояринцев, 2006] большое внимание уделено изучению опыта системного подхода к проектированию комплексов СФЗ, с единых системных позиций рассмотрены требования к СФЗ на основе анализа уязвимости, пути повышения эффективности управления СФЗ КВО. В работе достаточно подробно изложены методические подходы к категорированию объектов, определению количественных и качественных требований к СФЗ и оценке их эффективности.

Проблемам создания высокоэффективных систем охранно-пожарной сигнализации для нережимных объектов, а также интегрированных комплексов управления в системах безопасности объектов уделено внимание в работах [Магауенов, 2007; Синилов, 2010], систематизировавших наиболее сложные вопросы защиты объектов с помощью средств инженерно-технической укрепленности и технических средств охраны, а также типовые варианты их применения. В научных трудах [Измайлов, 2009; Боровский, Тарасов, 2011]

для различных категорий объектов описаны передовые подходы к построению их СФЗ, рассмотрены теоретические и практические вопросы интегральной оценки СФЗ, предложены методы их оптимизации.

Современные тенденции развития СОКБ КВО показывают, что фундаментальной основой таких систем служит единая аппаратно-программная платформа [Platzer, 2018], представляющая собой автоматизированную систему управления с многоуровневой сетевой структурой, имеющую общий центр управления на базе локальной компьютерной сети и содержащую линии коммуникаций, контроллеры доступа и другие устройства, предназначенные для сбора и обработки информации от различных периферийных средств обнаружения угроз (датчиков, сенсоров), а также для управления комплексами безопасности, автоматизации и жизнеобеспечения объекта [Garcia-Valls, 2017].

Таким образом, на современном этапе развития систем обеспечения безопасности критически важных объектов во все возрастающем темпе усложняются как структуры отдельных ее подсистем, так и системы в целом [Смирнов, Безручко, Басов, 2019]. Это относится как к функциональным подсистемам, обеспечивающим основные составляющие комплексной безопасности (см. рис. 1), так и к системам передачи и обработки тревожной информации, а также системе управления. Основные задачи и проблемы синтеза сложных систем, к коим в полной мере можно отнести и СОКБ, тесно взаимосвязаны и в своей совокупности образуют не решенную в полном объеме сложную проблему, интенсивно разрабатываемую в настоящее время многими исследователями: декомпозиции, агрегации и координации [Месарович, Такахара, 1973]; формализованного описания элементов сложной системы и их структурных взаимосвязей [Цвиркун, 1982]; управления структурной динамикой сложных технических систем [Охтилев, Соколов, Юсупов, 2005].

Исследование данных подходов показывает наличие достаточно тесной взаимосвязи между задачей синтеза СОКБ и задачами оптимизации функционирования системы в целом и отдельных ее подсистем [Офицеров, Еременко, Черепков, 2012]. При этом возможны два варианта решения: в первом случае для заданной совокупности функциональных подсистем СОКБ, а также элементов критически важного объекта и взаимосвязей между ними необходимо провести оптимизацию функционирования СОКБ для обеспечения максимальной безопасности объекта, во втором – для заданного уровня безопасности, определяемого категорией критически важного объекта, требуется произвести расчет и формирование оптимального состава подсистем СОКБ и входящих в них элементов, взаимосвязей между ними, а также рациональное распределение выполняемых задач и функций по элементам системы [Кащенко, Семенов, 2012].

Наименее исследованным на современном этапе подходом, но в то же время позволяющим наиболее точно определить набор конкретных элементов СОКБ, обеспечивающий требуемый уровень безопасности, является реализация метода синтеза структуры системы при заданных алгоритмах и принципах функционирования отдельных ее подсистем, в основу которого положен принцип последовательного синтеза моделей построения системы в целом (полимодельное представление), а также допустимых вариантов реализации функциональных подсистем и входящих в них элементов с последующим выбором на синтезируемых моделях наиболее эффективного варианта их реализации и развития. Данный подход позволит эффективно решить наиболее важные задачи синтеза структуры СОКБ, детализация которых обусловлена конкретными целями и этапом разработки системы [Офицеров, Еременко и др., 2011; Киселев, Мотиенко и др., 2018].

2. Применение агрегативно-декомпозиционного подхода для синтеза систем обеспечения комплексной безопасности критически важных объектов

Проведенные исследования в области проектирования СОКБ КВО показывают достаточно серьезную диспропорцию между интенсивным внедрением отдельных технических средств и комплексов охраны для объектов различных категорий и крайней разрозненностью их применения в совокупности с очень слабым привлечением для

разработки комплексных систем инновационных теоретических и практических наработок, что в итоге способно кардинально ослабить отдельные составляющие комплексной безопасности КВО: физической, территориальной, пожарной, психологической, информационной, экологической, радиационной и химической. Повышение знаний о СОКБ КВО в непрерывно изменяющихся условиях их функционирования, несмотря на некоторую неопределенность, определяет более высокую степень корректности решения задач по обеспечению комплексной безопасности данных объектов [Balaji, 2015].

Задачи синтеза структуры СОКБ могут быть поставлены для различных плоскостей (уровней) детализации построения системы на основе агрегативно-декомпозиционного подхода (рис. 2).

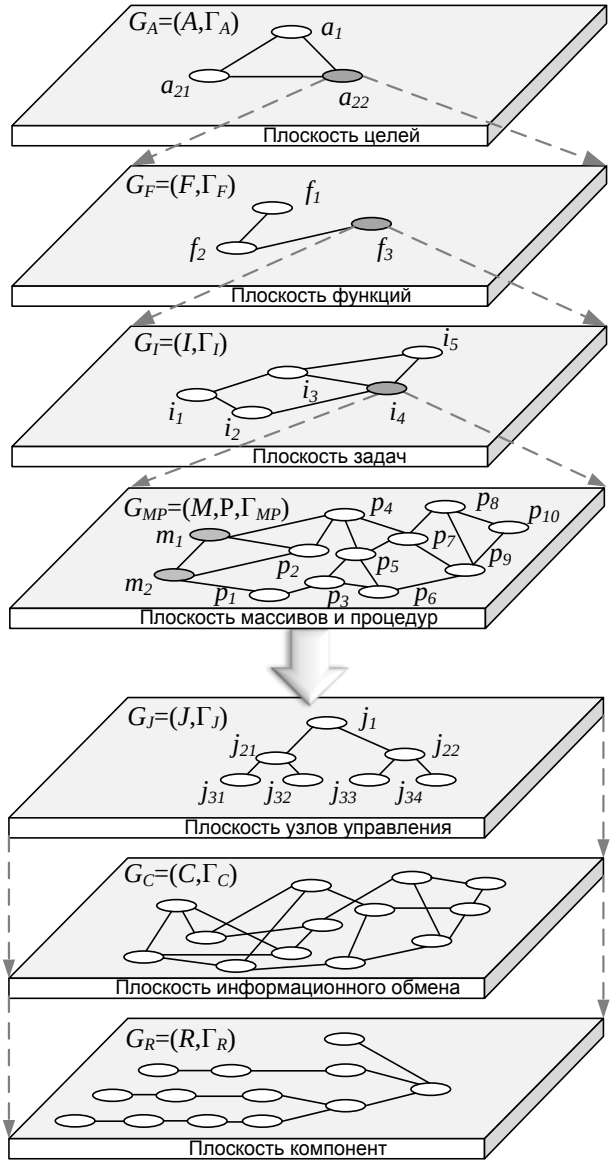

Рис. 2. Агрегативно-декомпозиционный подход к построению
систем обеспечения комплексной безопасности критически важных объектов
Fig. 2. The aggregative-decomposition approach to construction of complex safety maintenance systems on critical objects

Агрегативно-декомпозиционный подход включает два взаимосвязанных этапа: на первом этапе осуществляется последовательная декомпозиция реализуемых целей, функций, задач, массивов и процедур, в результате чего СОКБ представляется в виде упорядоченной совокупности взаимосвязанных функциональных подсистем и элементов

различной степени детализации; на втором – производится объединение (агрегирование) элементов с целью формирования возможных вариантов построения СОКБ КВО на соответствующем уровне (плоскости) детализации [Цвиркун, 1982]. При этом на верхнем уровне формализуются реализуемые системой цели, выполняемые функции и решаемые задачи, на более низких уровнях они детализируются до отдельных массивов и процедур. Возможные альтернативы агрегирования элементов в пределах функциональных подсистем, а также подсистем в СОКБ КВО в целом наиболее целесообразно представлять альтернативно-графовой формализацией с вершинами альтернативного графа в качестве вариантов построения функциональных подсистем (элементов) и дугами, обозначающими взаимосвязи между ними [Зыков, 2004].

Представленный на рисунке 2 граф $G_A = (A, \Gamma_A)$ задает взаимосвязи конечного множества вариантов реализуемых СОКБ КВО целей, где $A = \{a_1, a_{21}, a_{22}\}$ – множество вершин альтернативного графа, соответствующих уровням детализации выполняемых системой безопасности целей. Здесь в качестве метацели a_1 принята цель обеспечения комплексной безопасности критически важного объекта, в качестве целей второго уровня: a_{21} – безопасность материальных (информационных) ценностей на объекте, a_{22} – защита самого критически важного объекта. Множество дуг Γ_A на альтернативном графе отражает характер и специфику взаимосвязей между реализуемыми системой целями.

Представленный на рисунке 2 граф $G_F = (F, \Gamma_F)$ задает альтернативные варианты реализации СОКБ КВО функций, где $F = \{f_1, f_2, f_3\}$ – множество выполняемых системой функции (вершин альтернативного графа), Γ_F – множество логических взаимосвязей между функциями f_i (дуг графа), отражающих последовательность их реализации. Здесь в качестве функции f_1 примем анализ и прогнозирование угроз, f_2 – их обнаружение, f_3 – нейтрализацию. Элементы $G_F = (F, \Gamma_F)$ являются детализацией соответствующих вершин графа $G_A = (A, \Gamma_A)$.

Аналогично граф $G_I = (I, \Gamma_I)$ на рисунке 2 показывает альтернативные варианты решения задач, стоящих перед системой, при этом множество вершин графа $I = \{i_1, i_2, i_3, i_4, i_5\}$ отражает различные варианты реализации задач СОКБ, в той или иной мере обеспечивающих соответствующие составляющие комплексной безопасности (см. рис. 1). Здесь в качестве решаемых задач СОКБ предлагается обеспечение: i_1 – физической защиты, i_2 – психологической защиты, i_3 – экологической защиты, i_4 – техногенной защиты, i_5 – специальной защиты. Множество дуг графа Γ_I отражает характер взаимосвязей между решаемыми системой задачами. Здесь стоит отметить, что поскольку деление на задачи и функции во многом определяется особенностями конкретного объекта и спецификой применяемой на нем СОКБ, то оно является во многом относительным, в связи с чем принципы построения и структура графа $G_I = (I, \Gamma_I)$ аналогичны графу $G_F = (F, \Gamma_F)$.

Представленный на рисунке 2 граф $G_{MP} = (M, P, \Gamma_{MP})$ отражает альтернативные варианты реализации массивов $M = \{m_1, m_2\}$ и процедур

$$P = \{p_1, p_2, p_3, p_4, p_5, p_6, p_7, p_8, p_9, p_{10}\}.$$

С точки зрения реализации задач и функций СОКБ массивы представляют собой типовые части системы и соответствуют: m_1 – сотрудники охраны, m_2 – технические средства усиления охраны. В качестве процедур, реализуемых СОКБ на охраняемом объекте, предлагается

использовать способы и средства обеспечения безопасности: p_1 – дежурная служба, p_2 – постовая служба, p_3 – обходно-дозорная служба, p_4 – личная охрана, p_5 – охранная и тревожная сигнализация, p_6 – контроль доступа, p_7 – пожарная сигнализация, p_8 – охранное телевидение, p_9 – защита информации, p_{10} – жизнеобеспечение критически важного объекта. Важно отметить, что предлагаемый перечень массивов и процедур не является неизменным, обусловлен конкретными условиями оперативной обстановки и особенностями функционирования критически важного объекта, при этом множество дуг альтернативного графа Γ_{MP} определяет характер и особенности взаимосвязей как внутри множеств массивов *M* и процедур *P*, так и взаимодействие между элементами различных множеств.

Граф $G_J = (J, \Gamma_J)$ на рисунке 2 определяет альтернативные варианты применения узлов управления СОКБ (*J*), представленных на различных уровнях детализации. Множество дуг графа Γ_J отражает характер взаимосвязей между узлами управления на соответствующих уровнях.

Расположенные на нижних плоскостях структуры графы $G_C = (J, \Gamma_C)$ и $G_R = (J, \Gamma_R)$ определяют соответственно альтернативные варианты объединения сетевых устройств Γ_C в неблокируемую сеть передачи данных, а также альтернативные варианты взаимосвязей периферийных компонентов (сенсоры, извещатели, видеокамеры и т. д.), и могут быть детализированы до отдельных этапов и объектов процесса информационного обмена на различных уровнях (рис. 3).

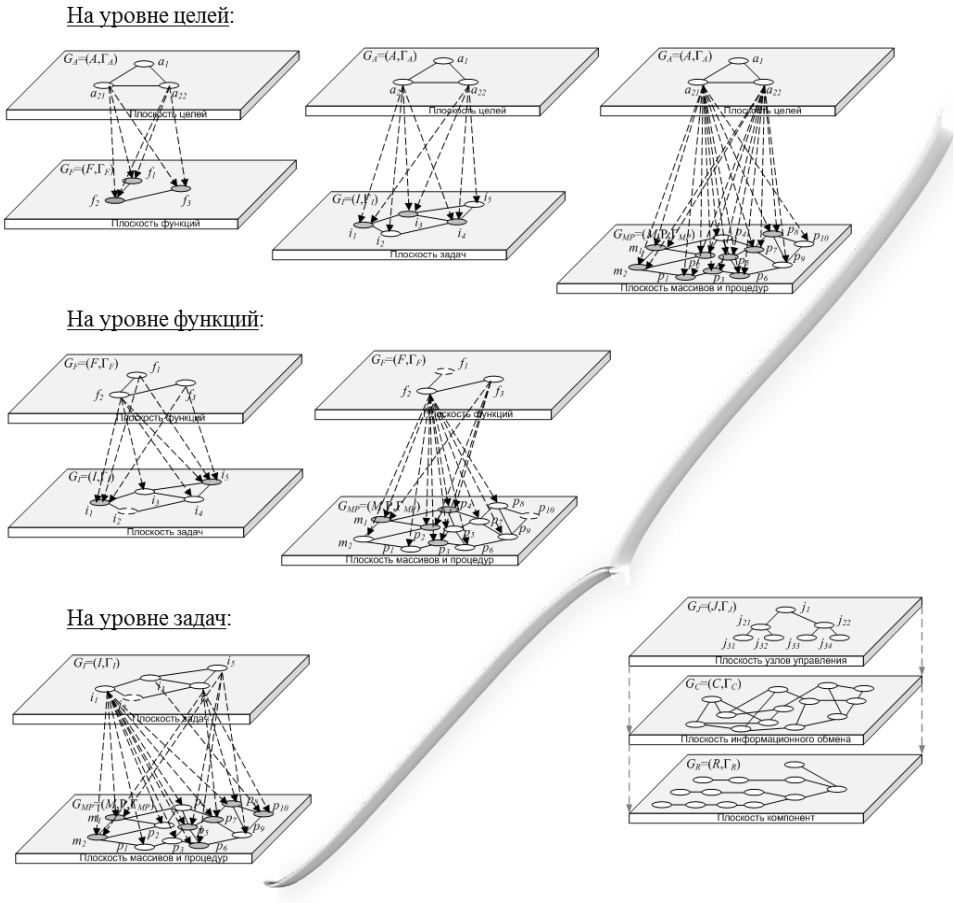

Рис. 3. Вариант агрегирования при построении систем обеспечения комплексной безопасности критически важных объектов

Fig. 3. Aggregation variant at construction of complex safety maintenance systems on critical objects

Агрегирование может осуществляться па различных уровнях (целей, функций, задач), а также различными способами, при этом характер агрегирования в большей степени определяется видом графов $G_J = (J, \Gamma_J)$ взаимосвязей между узлами управления, $G_C = (J, \Gamma_C)$ структуры сети передачи данных и $G_R = (J, \Gamma_R)$ взаимосвязей периферийных компонентов (рис. 3).

С учетом специфики построения СОКБ КВО соответствующие задачи агрегирования элементов системы могут быть сформулированы для любого из рассмотренных уровней (плоскостей) детализации описания СОКБ.

Таким образом, представленный в работе агрегативно-декомпозиционный подход к построению СОКБ КВО позволяет, в соответствии с требуемым уровнем детализации реализуемых системой целей, выполняемых функций и задач, решить ряд наиболее острых проблем синтеза структуры СОКБ КВО [Офицеров, Еременко и др., 2011; Цвиркун, 1982]:

1) оптимальное отображение множества выполняемых СОКБ КВО целей (граф $G_A = (A, \Gamma_A)$) на альтернативное множество узлов управления (граф $G_J = (J, \Gamma_J)$);

2) оптимальное отображение множества выполняемых СОКБ КВО функций, задач, массивов и процедур (графы G_F, G_I, G_{MP}) на плоскость информационного обмена (граф G_C);

3) оптимизация состава, вариантов реализации (функциональных подсистем) и размещения узлов системы (графы G_J, G_C, G_R).

Заключение

В связи с вышеизложенным, актуальность представленных исследований заключается в создавшихся предпосылках к изменению подходов в обеспечении безопасности критически важных объектов, отсутствии единых теоретических и методологических основ в данной предметной области и требует решения проблем, обусловленных двумя группами факторов [Басов, Ронжин, 2015].

Проблемы практики (первая группа факторов) – диспропорция между стремительно возрастающим и усложняющимся характером угроз критически важным объектам и ограниченными возможностями отдельных подсистем безопасности по противодействию этим угрозам, не обеспечивающими требуемого уровня защищенности объекта. Указанная диспропорция усугубляется еще и тем, что в ряде случаев при отдельном использовании подсистем безопасности, направленных на противодействие определенному направлению угроз и не учитывающих их комплексный характер, принятие мер по повышению эффективности одной подсистемы влечет снижение эффективности других подсистем, что в конечном счете приводит к снижению уровня защищенности объекта.

Проблемы теории (вторая группа факторов) – недостаточный теоретический и методологический уровень развития основ решения задач анализа, синтеза и оптимизации характеристик СОКБ КВО и их элементов. Указанная недостаточность проявляется прежде всего в несоответствии современным угрозам и узкой специализации инструментария анализа и синтеза отдельных подсистем безопасности, не учитывающего их взаимного влияния и комплексного характера использования в составе единой системы обеспечения комплексной безопасности.

Преодоление указанных противоречий требует разработки новых элементов теории построения систем обеспечения комплексной безопасности критически важных объектов.

Список литературы

1. Басов О.О., Ронжин А.Л. 2015. Методика поэтапного внедрения полимодальных инфокоммуникационных систем. Научные ведомости Белгородского государственного университета. 1 (198): 131–136.

2. Боровский А.С., Тарасов А.Д. 2011. Общая математическая модель системы физической защиты объектов. Вестник компьютерных и информационных технологий. 10 (88): 21–29.

3. Боровский А.С. 2013. Обоснование требований (показателей качества) к оценке защищенности потенциально-опасных объектов. Вестник компьютерных и информационных технологий. 7 (109): 52–56.

4. Боровский А.С. 2015. Модели, методы и алгоритмы интеллектуальной поддержки принятия решений в задачах разработки и оценки систем физической защиты объектов информатизации. Дисс. … докт. тех. наук. Оренбург. 344.

5. Бояринцев А.В., Бражник А.Н., Зуев А.Г. 2006. Проблемы антитерроризма: категорирование и анализ уязвимости объектов. СПб., Иста-Системс, 251.

6. Гарсиа М. 2002. Проектирование и оценка систем физической защиты: пер. с англ. М., Мир, АСТ, 386.

7. Зыков А. А. 2004. Основы теории графов. М., Вузовская книга, 664.

8. Кащенко А.Г., Семенов Р.В. 2012. Методика решения нечетких многокритериальных задач выбора вариантов информационно-телекоммуникационных систем. Научные ведомости Белгородского государственного университета. Серия: История. Политология. Экономика. Информатика. 19 (138), Вып. 24/1: 161–164.

9. Киселев Ю.В., Мотиенко А.И., Басов О.О., Саитов И.А. 2018. Структурно-функциональная модель интеллектуальной инфокоммуникационной системы. Научно-технический вестник информационных технологий, механики и оптики. 18 (6): 1034–1046.

10. Магауенов Р.Г. 2007. Охранная сигнализация и другие элементы систем физической защиты: Краткий толковый словарь. М., Горячая линия – Телеком, 97.

11. Месарович М., Мако Д., Такахара Я. 1973. Теория иерархических многоуровневых систем. М., Мир, 344.

12. Офицеров А.И. Еременко В.Т., Черепков С.А. 2012. Метод проектирования сетей передачи данных, совместимых с неблокируемой маршрутизацией. Вестник компьютерных и информационных технологий. 4: 38–46.

13. Офицеров А.И., Еременко В.Т., Афонин С.И., Басов О.О. 2011. Синтез сетей передачи данных автоматизированных систем управления на основе критерия неблокируемой маршрутизации. Научные ведомости Белгородского государственного университета. Серия: История. Политология. Экономика. Информатика. 7 (102). Вып. 18/1: 168–176.

14. Охтилев М.Ю., Соколов Б.В., Юсупов Р.М. 2005. Интеллектуальные технологии мониторинга состояния и управления структурной динамикой сложных технических объектов. М., Наука, 291.

15. Саати Т. 1993. Принятие решений. Метод анализа иерархий. Перевод с английского Р.Г. Вачнадзе. М., Радио и связь, 278.

16. Смирнов А.В., Безручко В.В., Басов О.О. 2019. Теоретические основы построения социокиберфизических систем. Научные ведомости Белгородского государственного университета. Серия: Экономика. Информатика. 46 (3): 532–539.

17. Цвиркун А.Д. 1982. Основы синтеза структуры сложных систем. М., Наука, 200.

18. Balaji B. 2015. Models, abstractions, and architectures: The missing links in cyber-physical systems. Proceedings of the 52nd Annual Design Automation Conference, San Francisco, CA, USA. 8–12 June 2015; New York, NY, USA: 82–87.

19. Garcia-Valls M. 2017. Reliable software technologies and communication middleware: A perspective and evolution directions for cyber-physical systems, mobility, and cloud computing. Future Gener. Comput. Syst., 71:171–176.

20. Platzer A. 2018. Logical Foundations of Cyber-Physical Systems. Springer, 662.

References

1. Basov O.O., Ronzhin A.L. 2015. Technique of phased implementation of polymodal communication systems. Belgorod State University Scientific Bulletin. 1 (198): 131–136. (in Russian).

2. Borovskij A.S., Tarasov A.D. 2011. General mathematical model of the physical protection system of objects. Vestnik komp`yuternyh i informatsionnyh tekhnologiy. 2011. 10 (88): 21–29. (in Russian).

3. Borovskij A.S. 2013. Justification of requirements (quality indicators) for the assessment of the protection of potentially dangerous objects. Vestnik komp`yuternyh i informatsionnyh tekhnologiy. 7 (109): 52–56. (in Russian).

4. Borovskij A.S. 2015. Modeli, metody i algoritmy intelektual`noi` podderzhki prinyatiya reshenii` v zadachah razrabotki I ocenki system fizicheskoi` zashchity ob`ektov informatizacii [Models, methods and

algorithms of intellectual decision-making support in the tasks of developing and evaluating physical protection systems of informatization objects]. Diss. … dr. sci. tech. Orenburg. 344.

5. Boyarintsev A.V., Brazhnik A.N., Zuev A.G. 2006. The problems of anti-terrorism: categorization and analysis of the vulnerability of objects. SPb., Ista-Systems, 251. (in Russian).

6. Garcia M. 2002. Design and evaluation of physical protection systems: trans. from English M., World, AST, 386. (in Russian).

7. Zykov A. A. 2004. Fundamentals of graph theory. M., University Book, 664. (in Russian).

8. Kashchenko A.G., Semenov R.V. 2012. Methodology for solving fuzzy multi-criteria problems of choosing options for information and telecommunication systems. Scientific reports of Belgorod State University. Series: History. Political science. Economy. Computer science. 19 (138), no. 24/1: 161–164. (in Russian).

9. Kiselev Yu.V., Motienko A.I., Basov O.O., Saitov I.A. 2018. Structural-functional model of inteIligent infocommunication system. Scientific and Technical Journal of Information Technologies, Mechanics and Optics. 18 (6): 1034–1046. (in Russian).

10. Magauenov R.G. 2007. Security Alarms and Other Elements of Physical Protection Systems: A Brief Explanatory Dictionary. M., Hotline – Telecom, 97. (in Russian).

11. Mesarovich M., Mako D., Takahara Y. 1973. The theory of hierarchical multilevel systems. M., World, 344. (in Russian).

12. Ofitserov A.I., Eremenko V.T., Tsherepkov S.A. 2012. Method for providing lock-free routing in designing a data network. Vestnik komp`yuternyh i informatsionnyh tekhnologiy. 4: 38–46. (in Russian).

13. Ofitserov A.I., Eremenko V.T., Afonin S.I., Basov O.O. 2011. Syntheses of the data networks of automated management systems on base of criterion of the unlockable routing, Belgorod State University Scientific Bulletin, History Political Science Economics Information technologies. 7(102), no. 18/1: 168–176. (in Russian).

14. Okhtilev M.Yu., Sokolov B.V., Yusupov R.M. 2005. Intelligent technologies for monitoring the state and controlling the structural dynamics of complex technical objects. M., Science, 291. (in Russian).

15. Saati T. 1993. Making decisions. Hierarchy analysis method. Translation from English by R.G. Vachnadze. M., Radio i svjaz', 278.

16. Smirnov A.V., Bezruzhko V.V., Basov O.O. 2019. Theoretical bases of the construction of cyber-physical system development. Belgorod State University Scientific Bulletin. Economics. Information technologies. 46 (3): 532–539 (in Russian).

17. Zvirkun A.D. 1982. Fundamentals of the synthesis of the structure of complex systems. M., Science, 200. (in Russian).

18. Balaji B. 2015. Models, abstractions, and architectures: The missing links in cyber-physical systems. Proceedings of the 52nd Annual Design Automation Conference, San Francisco, CA, USA. 8–12 June 2015; New York, NY, USA: 82–87.

19. Garcia-Valls M. 2017. Reliable software technologies and communication middleware: A perspective and evolution directions for cyber-physical systems, mobility, and cloud computing. Future Gener. Comput. Syst., 71:171–176.

20. Platzer A. 2018. Logical Foundations of Cyber-Physical Systems. Springer, 662.

Ссылка для цитирования статьи
For citation

Офицеров А.И., Басов О.О., Бачурин С.С. 2020. Концептуальные основы обеспечения комплексной безопасности критически важных объектов. Экономика. Информатика. 47 (1): 154–163. DOI:

Ofitserov A.I., Basov O.O., Batchurin S.S. 2020. Conceptual bases of maintenance of complex safety on critical objects. Economics. Information technologies. 47 (1): 154–163 (in Russian). DOI: