Процессные аспекты нормативного регулирования работ по комплексному обеспечению информационной безопасности и интероперабельности интегрированных систем управления

А.А. Зацаринный, email: azatsarinny@ipiran.ru
С.В. Козлов, email: sv_kozlov@mail.ru

Федеральное государственное учреждение
«Федеральный исследовательский центр «Информатика и управление»
Российской академии наук»

Аннотация. *Создание и развитие интегрированных систем управления направлено на обеспечение их адекватного реагирования на угрозы и опасности в сфере деятельности органов государственного и корпоративного управления. По мере развития технологий, применяемых при их создании, одновременно расширяются горизонты внешних и внутренних угроз и опасностей. В статье рассматриваются основные проблемы обеспечения информационной безопасности интегрированных систем управления на начальных стадиях их жизненного цикла, связанные с деятельностью субъектов государственного заказа при обосновании и реализации системотехнических и технологических решений по их созданию. Показано, что с ростом технологической сложности перспективных интегрированных систем и расширением их функциональности проявляется комплексная проблема интероперабельности и информационной безопасности, трансформируется и предмет их исследования, при этом приобретает высокую актуальность переход от системотехники к системной инженерии в жизненном цикле интегрированных систем. Представлены основные направления нормативного регулирования такой комплексной проблемы на уровне национальных стандартов, гармонизированных с международными стандартами и рекомендациями.*

Ключевые слова: *Интегрированная система управления, комплексная проблема интероперабельности и информационной безопасности, системная инженерия, нормативное регулирование, национальные стандарты*

Введение

Современные тенденции развития интегрированных систем управления различного назначения (ИСУ) с реализацией

© Зацаринный А.А., Козлов С.В., 2021

сетецентрических принципов связаны с необходимостью обеспечения их инвариантности ИСУ к широкому перечню угроз и опасностей в сфере ответственности конкретной системы управления в условиях объективных процессов по расширению их функциональности. При этом применение в составе ИСУ новых функциональных подсистем и комплексов в виде совокупности управляющих и исполнительных систем, создаваемых на основе перспективных информационных технологий, выводит проблему повышения качества ИСУ на новый уровень. Все более востребованным становится анализ проблем на стыке функциональных систем с выявлением уязвимостей и обоснованием мер по их устранению. В этой связи применительно к области многофункциональных систем на первый план выдвигается комплексная проблема обеспечения интероперабельности и информационной безопасности. В организационном плане эта проблема должна решаться совместными усилиями всех субъектов государственного заказа, начиная с ранних этапов подготовки заказа на проектирование системы.

До настоящего времени нормативное регулирование работ по созданию автоматизированных систем на основе информационных технологий обеспечивается, в основном, в соответствии с государственными стандартами 34 серии. Вместе с тем, многие вопросы разработки автоматизированных систем управления как многофункциональных систем находятся вне сферы нормативного регулирования, а такие межсистемные проблемы, как интероперабельность многофункциональных систем и информационная безопасность, требуют безотлагательного принятия мер по их идентификации и регулированию на уровне национальных стандартов.

1. Уточнение парадигмы исследования интегрированной системы управления

Ретроспективный анализ систем управления различного назначения позволяет условно выделить в их развитии несколько стадий, как показано на рис. 1 и в таблице:

- узкоспециализированные системы, направленные на реализацию нескольких разобщенных функций в условиях достаточной степени определенности применения системы управления;
- комплексные системы, реализующие процессы информатизации органов управления и автоматизации деятельности их должностных лиц (по существу, это была первая стадия классической интеграции по принципу: новые задачи – новая структура системы управления);

– интеграция систем на основе наращивания функциональных возможностей комплексных систем управления с использованием готовых к совместному применению новых функциональных подсистем (например, подсистем навигации, ориентирования, опознавания и др.) на базе системы CASE-технологий;
– интеграция систем на уровне бизнес-процессов;
– интеграция систем на основе процессного подхода с учетом увеличения перечня рассматриваемых процессов в жизненном цикле системы управления.

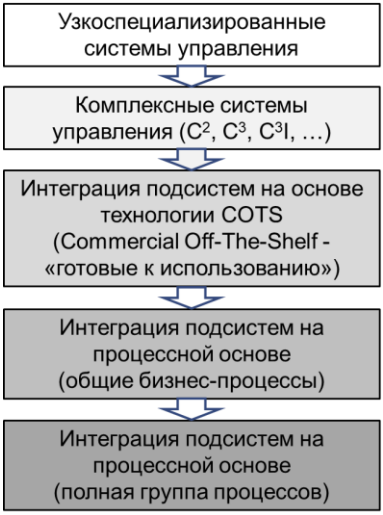

Рис. 1. Эволюция от монофункциональных систем до интегрированных многофункциональных систем управления

На основе такого представления ретроспективы развития систем управления как объектов исследования и разработки можно показать эволюцию объекта и предмета исследования по такой тематике работы.

Таблица

Эволюция объекта и предмета исследований по тематике интегрированных систем управления

Стадии интеграции элементов системы управления	Основные признаки стадии интеграции	Предмет исследования	Методы исследования
Типовой объект исследования (на 1-й и 2-й стадии интеграции элементов)	Система управления как взаимоувязанная совокупность органов, центров управления и средств управления	Бизнес-процессы в жизненном цикле. Системотехника	Функциональный подход к созданию ИСУ. Системная инженерия.
Современный объект исследования (на 3-й стадии интеграции элементов)	ИСУ как много-функциональная система на уровне органов, центров и средств управления	Полная группа процессов в жизненном цикле.	Процессный и проектный подходы. Системная инженерия.

Так, например, на 1-й и 2-й стадиях интеграции система управления как объект исследования, представляется в виде взаимоувязанной совокупности органов, центров и средств управления. а предмет исследования составляют бизнес-процессы и системотехника для их реализации. Основными методами исследований являются методы функционального подхода и системной инженерии.

В настоящее время возрастает актуальность объекта исследования в виде интегрированной системы управления как многофункциональной системы на уровне элементов системы управления, рассматриваемых на второй стадии. При этом предмет исследования должен рассматриваться практически полностью на уровне процессов в жизненном цикле системы управления, а методы исследования – на основе процессного и проектного подходов и системной инженерии.

Еще четверть века тому назад такая интеграция ограничивалась тремя, максимум четырьмя видами функциональных систем, а обеспечение их совместного функционирования достигалось за счет применения системы протоколов и различного рода шлюзов. Дальнейшее расширение функциональности интегрированных систем

приводило к возрастанию сложности обеспечения совместимости их компонентов, а одновременное развитие противодействующих факторов, порой опережающее развитие интегрированных систем, становилось серьезным препятствием на пути повышения эффективности управленческой деятельности органов управления.

Инфокоммуникационная сфера в настоящее время является весьма уязвимой в отношении современных угроз и прогнозируемых опасностей. По мере развития технологий наблюдается интенсивное расширение горизонтов угроз, рост объемов разнородной, а часто и противоречивой информации о текущих угрозах. Складывается противоречивая ситуация, в которой в условиях нарастания внешних угроз лавинообразно растет сложность организации и обеспечения эффективной деятельности органов управления, что становится причиной появления и вторичных угроз внутрисистемного порядка.

Существующие ограничения системного подхода [1], связанные с недостаточной определенностью предметной сферы проведения исследований, с непротиворечивостью исходных данных и целостностью рассматриваемого объекта исследований, проявляются в том, что создаваемые изделия не в полной мере будут соответствовать условиям их применения. Учитывая особую важность управления во всех сферах жизни и деятельности личности, общества и государства и высокую сложность создаваемых современных систем управления различного назначения, такое положение становится сдерживающим фактором при создании многофункциональных интегрированных систем управления.

2. Основные направления нормативного регулирования работ по комплексному обеспечению информационной безопасности и интероперабельности интегрированных систем управления

Анализ основных угроз информационной безопасности интегрированных систем управления свидетельствует о том, что применительно к ним наибольшей уязвимостью обладает гетерогенная инфокоммуникационная среда, являющаяся основой создания и функционирования систем, формирование которой должно осуществляться с учетом обеспечения интероперабельности функциональных систем в их составе [2-5]. Учитывая высокую степень неопределенности при обеспечении информационной безопасности гетерогенных инфокоммуникационных систем, ее решение целесообразно осуществлять взаимоувязанно в комплексе с обеспечением интероперабельности разнородных функциональных систем, реализуемой на организационном, семантическом, техническом и нормативном уровнях. Нормативное регулирование общих вопросов

обеспечения интероперабельности осуществляется в соответствии с ГОСТ Р 55062-2012, в котором определены терминология и основные этапы обеспечения интероперабельности. В отношении первых трех уровней в настоящее время ведутся работы по разработке «Концепция обеспечения интероперабельности сетецентрических управляющих систем» и «Модели для построения и оценки интероперабельности сетецентрических управляющих систем» [6]. Документы оформлены, как проекты Рекомендаций по стандартизации Росстандарта и предназначены для использования субъектами госудпоственного и муниципального заказа при создании высокотехнологичных автоматизированных систем. Согласно ГОСТ Р 1.10-2004 Рекомендации по стандартизации разрабатываются в случае целесообразности предварительной проверки на практике неустоявшихся и еще не ставших типовыми организационно-методических положений в соответствующей области, т.е. до принятия национального стандарта Российской Федерации, в котором могут быть установлены эти положения.

Работы по разработке и гармонизации национальных стандартов по информационной безопасности информационных технологий ведутся в соответствии с Программой национальной стандартизации, и в настоящий период (2019-2021 гг.) ФИЦ ИУ РАН проводится разработка, гармонизация и подготовка к утверждению стандартов в области информационной безопасности и защиты информационных технологий с учетом современных тенденций их развития, в том числе, обработки массивов больших данных, реализующих облачные, туманные, квантовые технологии, технологии виртуальной и дополненной реальности и искусственного интеллекта.

Целью работы является поддержание национального фонда стандартов в области информационной безопасности и защиты информационных технологий на современном научно-техническом уровне, разработка и подготовка к принятию наиболее актуальных стандартов в этой области.

В рамках упомянутой работы проводятся разработка, публичное обсуждение, согласование и представление на утверждение проектов 71 стандарта, распределенных по трем группам, как показано на рис. 2. В ходе публичного обсуждения проектов стандартов основные замечания и рекомендации по их первой редакции поступают от следующих профильных технических комитетов по стандартизации:

- ТК22 «Информационные технологии»;
- ТК164 «Искусственный интеллект»;
- ТК228 «Средства надежного хранения и безопасности»;

– ТК362 «Защита информации».

Кроме того, в проведении экспертизы участвуют комитеты Торгово-промышленной палаты РФ по промышленной безопасности и безопасности предпринимательской деятельности, научно-исследовательские институты и другие заинтересованные организации.

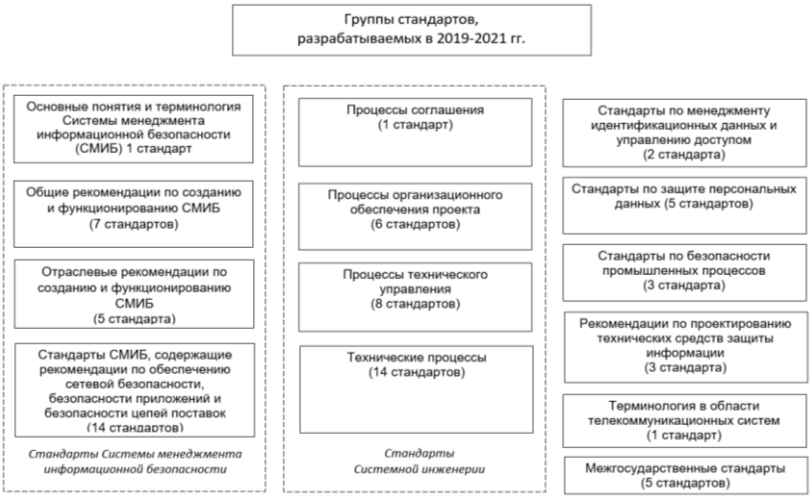

Рис. 2. Классификация разрабатываемых стандартов по тематике информационной безопасности.

В 2020 году завершена разработка, публичное обсуждение, согласование и утверждение приказом Федерального агентства по техническому регулированию и метрологии 10 стандартов, разработанных в качестве идентичных международным стандартам с учетом национальных особенностей регулируемой ими сферы:

- ГОСТ Р ИСО/МЭК 19086-4. Информационные технологии. Облачные вычисления Основы соглашения для уровня услуг Часть 4 Компоненты безопасности и защиты персональной информации (ISO/IEC 19086-4:2019, IDT);
- ГОСТ Р ИСО/МЭК 27010. Информационные технологии. Методы и средства обеспечения безопасности Управление информационной безопасности для связи между подразделениями и организациями (ISO/IEC 27010:2015, IDT);
- ГОСТ Р ИСО/МЭК 27018. Информационные технологии. Методы и средства обеспечения безопасности. Свод норм и правил по применению общедоступного облачного процессора

с расширенным управленческим набором для защиты персональной информации
- ГОСТ Р ИСО/МЭК 27033–6 Информационные технологии. Методы и средства обеспечения безопасности. Сетевая безопасность Часть 6 Защищенный доступ к беспроводной IP-сети (ISO/IEC 27033-6:2016, IDT);
- ГОСТ Р ИСО/МЭК 27034-5. Информационные технологии. Методы и средства обеспечения безопасности. Безопасность приложений. Часть 5 Протоколы и структура данных по средствам контроля для защиты приложений (ISO/IEC 27034-5:2017, IDT);
- ГОСТ Р ИСО/МЭК 27034-7. Информационные технологии. Безопасность приложений. Часть 7. Основы прогнозирования гарантии безопасности (ISO/IEC 27034-7:2018, IDT);
- ГОСТ Р ИСО/МЭК 27036-2. Информационные технологии Информационная безопасность во взаимоотношениях с поставщиками Часть 2. Требования (ISO/IEC 27036-2:2014, IDT).
- ГОСТ Р ИСО/МЭК 27036-3. Информационные технологии. Методы и средства обеспечения безопасности информационная безопасность во взаимоотношениях с поставщиками. Часть 3. Руководящие указания по безопасности информационных и коммуникационных технологий цепи поставок (ISO/IEC 27036-3:2013, IDT);
- ГОСТ Р ИСО/МЭК 27036-4. Методы и средства обеспечения безопасности. Информационная безопасность во взаимоотношениях с поставщиками Часть 4 Руководящие указания по безопасности облачных услуг (ISO/IEC 27036-4:2013, IDT);
- ГОСТ Р ИСО/МЭК 21878. Информационные технологии. Методы и средства обеспечения безопасности. Руководящие указания по обеспечению безопасности при проектировании и реализации виртуализированных серверов (ISO/IEC 21878:2019, IDT).

В перечне разрабатываемых стандартов в области безопасности информационных технологий (см. рис. 2) одна из групп включает стандарты по системной инженерии, определяющей логическую взаимосвязь в рамках деятельности всех субъектов государственного и муниципального заказа по обеспечению безопасности информационных технологий, применяемых при создании интегрированных систем управления. Важно отметить, что стандарты по тематике системной

инженерии регламентируют организационные и организационно-ресурсные процессы в области обеспечения информационной безопасности на протяжении жизненного цикла интегрированных систем управления. При этом в Программе национальной стандартизации выделены следующие направления стандартизации в области системной инженерии:

1. Стандартизация процессов соглашения (процессы приобретения и поставки).
2. Стандартизация процессов организационного обеспечения проекта (процессы управления моделью жизненного цикла, управления инфраструктурой, портфелем заказов, человеческими ресурсами, конфигурацией, информацией, измерениями и гарантии качества).
3. Стандартизация технических процессов (процессы анализа назначения, определения потребностей заинтересованных сторон, определения системных требований, архитектуры, проекта, системного анализа, реализации, комплексирования, верификации, передачи, валидации, функционирования, сопровождения, изъятия и списания).

Целью разработки стандартов по указанным группам является привязка стандартов к процессам системной инженерии, относящимся к обеспечению информационной безопасности интегрированных систем управления. Такой подход позволяет их использовать как автономно при разработке отдельных процессов в жизненном цикле систем, так и в комплексе с другими стандартами. В этой связи обеспечивается возможность комплексного нормативного регулирования процессов обеспечения интероперабельности и информационной безопасности в жизненном цикле интегрированных систем управления.

Заключение

В области создания интегрированных систем управления на основе объединения на качественно новой технологической основе автономных функциональных систем основным сдерживающим фактором является комплексная проблема интероперабельности и информационной безопасности, масштабы которой растут по мере расширения состава интегрированной системы.

Разобщенные подходы к решению такой проблемы, широко применяемые в практике заказчиков и разработчиков современных систем управления, приводят к непропорциональному росту новых проблем, связанных с появлением новых уязвимостей, порождающих дополнительные угрозы информационной безопасности интегрированных систем.

Дополнение Программы национальной стандартизации в России в части разработки и гармонизации национальных стандартов в области информационной безопасности стандартами в части регулирования вопросов интероперабельности интегрированных систем на основе сетецентрических принципов позволяет провести комплексную и взаимоувязанную разработку стандартов по интероперабельности на основе разрабатываемых стандартов в области информационной безопасности. При этом обеспечение взаимоувязанной их разработки целесообразно осуществлять на основе стандартов в области системной инженерии, определяющих процессную основу обеспечения информационной безопасности интегрированных систем управления на протяжении всех стадий их жизненного цикла

Статья подготовлена при поддержке грантов РФФИ № 19-07-00774 и № 18-29-03124

Список литературы

1. Пригожин, А. И. Методы развития организаций. -М.: МЦФЭР. − 2003. − 864 с.

2. Comparative performance evaluation of modern heterogenous high-performance computing CPUS / A. Sorokin [и др.] // Electronics (Switzerland). − 2020. W. 9. № 6. − pp. 1-13.

3. Зацаринный, А.А. Алгоритмы управления сервис-ориентированными процессами детерминированных научных сервисов в гибридных вычислительных средах цифровых платформ / А.А. Зацаринный, В.А. Кондрашев, Сорокин А.А. // Системы высокой доступности. − 2020. Т. 16. № 3. − С. 5−17.

4. Подход к обеспечению интероперабельности в сетецентрических системах управления / А. А. Башлыкова [и др.] // Журнал радиоэлектроники [электронный журнал]. − 2020. №6. Режим доступа: http://jre.cplire.ru/jre/jun20/13/ abstract.html

5. Информационное пространство цифровой экономики России. Концептуальные основы и проблемы формирования / А. А. Зацарииный, [и др.] // ФИЦ ИУ РАН. Изд-во ООО «НИПКЦ Восход-А», − М., 2018, − 236 с.

6. Олейников, А. Я. Основные положения концепции обеспечения интероперабельности сетецентрических информационно-управляющих систем / А. Я. Олейников, Д. В. Растягаев, И. А. Фомин. // Вестник Российского нового университета: серия сложные системы, модели, анализ и управление. − 2020. Выпуск №3. − С. 122-131.