УДК 004.052.3

о НЕОБХОДИМОСТИ СОПРОВОЖДЕНИЯ СТАНДАРТАМИ МЕТОДИКИ САМОВОССТАНОВЛЕНИЯ КРИТИЧЕСКОГО СЕГМЕНТА РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

**1,2 Башлыкова А.А.**

1Федеральное государственное бюджетное образовательное учреждение высшего образования «МИРЭА - Российский технологический университет», 119454, Россия, г. Москва, проспект Вернадского, 78, e-mail:
bashlykova\_a\_a\_mirea@mail.ru

2Федеральное государственное бюджетное учреждение науки «Институт радиотехники и электроники им. В.А.Котельникова РАН (ИРЭ им.В.А.Котеьникова РАН), 125009, Россия, Москва, ул. Моховая 11, корп.7.

Требования к специфичным и критическим сегментам распределенных информационных систем, не получают отражение в профилях и стандартах, а формируются на уровнях решения задач в каждой конкретной системе. Построенная распределенная информационная система с критическим сегментом, на основе работы вычислительной сети, должна решать задачи, связанные со сбором данных из разнесённых узлов и их агрегированием. При разработке проекта Студенческой научной группы отмечен недостаток сопровождения реализации критических сегментов, и необходимость составления профиля.

Ключевые слова: профиль, стандарт, критический сегмент, распределенная информационная система, интероперабельность.

ABOUT THE NECESSITY of accompaniment by STANDARDS, METHODS OF SELF-HEALING OF A CRITICAL SEGMENT OF DISTRIBUTED INFORMATION SYSTEMS

**1,2 Bashlykova A.A.**

*1Federal State Educational Institution of Higher Education “MIREA - Moscow technological university”, 119454, Russia, Vernads avenue, 78, Moscow e-mail:* *bashlykova\_a\_a\_mirea@mail.ru*

*2Federal State Budgetary Institution of Science Kotelnikov Institute of Radioengineering and Electronics (IRE) of Russian Academy of Sciences, 125009, Russia, Mokhovaya 11-7, Moscow.*

Requirements for specific and critical segments of distributed information systems are not reflected in profiles and standards, but are formed at the levels of problem solving in each specific system. The constructed distributed information system with a critical segment, based on the work of the computer network, should solve the problems associated with the collection of data from the separated nodes and their aggregation. In the development of the project of the Student scientific group noted the lack of support for the implementation of critical segments, and the need to compile a profile.

Key words: profile, standard, critical segment, distributed information system, interoperability.

**Введение**

В настоящее время концепции построения распределенных информационных систем насчитывает большое множество технологий для их реализации, к примеру, реализации на основе протоколов Z39.50, SRU/SRW и пришедшие им на смену протоколы.

Стандартизировать структуру информационной системы (ИС) подходы *ITSM*, *ITIL* и стандарты группы ISO для управления ИС в той сфере, в которой она реализуется. Среди требований, предъявляемых к распределенным информационным системам (РИС), можно выделить следующие четыре основных:

- интероперабельность;

- прозрачность;

- масштабируемость;

- надёжность.

Сбой в работе сегмента вычислительной сети (ВС), лежащей в транспортной основе, ощутимо отразится на работе всей РИС предприятия, вплоть до полного прекращения функционирования. Поэтому узловые элементы сегмента ВС должны обладать свойством восстанавливаемость, заключающемся в способности восстанавливаться после отказа без ремонта [1].

В вычислительной сети (ВС), как взаимосвязанной совокупности территориально рассредоточенных систем обработки данных, средств и (или) систем связи и передачи данных, обеспечивающей пользователям дистанционный доступ к ее ресурсам и коллективное использование этих ресурсов [2], можно выделить домен отказа – область сети, на которую оказывают воздействие сбои в работе критически важного устройства или сетевого сервиса.

Критический сегмент (КС) РИС, функционирующей на основе ВС, можно рассматривать как подсистему информационной инфраструктуры (ИИ), включающую в себя физические и виртуальные средства и системы, сбой в работе которых или уничтожение приводит к серьёзным негативным последствиям [8,9].

**Цель исследования – критический сегмент распределенной информационной системы. Требования стандартов.**

Согласно федеральному закону "О безопасности критической информационной инфраструктуры Российской Федерации" [7], вступившему в силу 1 января 2018 года, наличие в инфраструктуре критического сегмента позволяет отнести эту инфраструктуру к критической.

Из закона "О безопасности критической информационной инфраструктуры Российской Федерации" следует, что сегмент считается критическим, если он содержит ИС, телекоммуникационную сеть либо автоматизированную систему управления (АСУ) технологическими процессами [7]. Критическая ИИ – объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов [7].

В методических указаниях, утверждённых МЧС, «Методика отнесения объектов государственной и негосударственной собственности к критически важным объектам для национальной безопасности Российской Федерации» [11] приводятся группы объектов государственной и негосударственной собственности, которые содержат критический сегмент, нарушение функционирования которого может серьёзно сказаться на национальной безопасности страны. К числу таких групп, согласно документу, относятся: организации оборонно-промышленного комплекса, организации с числом сотрудников, превышающим 10 тыс. человек, организации-монополии, объекты информационной и телекоммуникационной инфраструктуры и др.

Основные определения и термины, связанные с КИИ и её объектами, даны в федеральном законе "О безопасности критической информационной инфраструктуры Российской Федерации" [7]. Из этого закона и из методических указаний [11] следует, что идентифицированными как критические сегменты могут быть информационные и телекоммуникационные системы и сети:

органов государственной власти различных уровней (Правительство РФ, Верховный Суд РФ); предприятий и организаций транспорта (например, ГУП «Мосгортранс»); банковской и финансовой сферы (например, Сбербанк ); организаций критически опасных производств (Росатом); водоснабжения (например, Мосводоканал); предприятий и организаций нефтегазовой отрасли (например, Роснефть, Лукойл); предприятий и организаций электроснабжения; сферы науки; сферы здравоохранения (например, Департамент здравоохранения города Москвы) и др.

**Недостаточность в стандартах и доступных профилях.**

На Рис. 1 отображены группы стандартов, которые можно рассматривать как документы, содержащие требования к КС РИС и как предстоящую основу разрабатываемого профиля.

Группировка требований к системе в целом указана в ГОСТ 34.602-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы», но специфика наличия критического сегмента и подобного, там нет.

Определение термина «восстанавливаемость» приводится в ГОСТ 27.002-2015 [1], согласно которому это свойство объекта, заключающееся в его способности восстанавливаться после отказа без ремонта. Под самовосстановлением будет пониматься свойство объекта, заключающееся в его способности восстанавливать работоспособность автоматически с минимальной задержкой, так чтобы с системной точки зрения сбой в работе КС РИС не происходил, то есть для РИС сбой КС прошёл незамеченным.

Следует отличать существующие методы самовосстановления в зависимости от объекта восстановления. Объектами аварийного восстановления являются сервисы ВС или ИС. Для локализации домена отказа, вызванного сбоем работы устройства критического сегмента, возможно произвести сегментирование КС – распределение функций КС между несколькими устройствами, расположенными в разрозненных локальных сетях, то есть обеспечить распределённую обработку данных. Это позволит уменьшить домен отказа и избежать полной потери работоспособности системы, в случае если сбой произойдёт только в одном сегменте КС.

Несмотря на то, что избыточность и сегментирование КС существенно повышают надёжность КС, данные методы не гарантирую 100% вероятности отсутствия отказов в КС РИС.

**Результат исследования**

Методика (Рис.2.) включает в себя три основных этапа:

* + - 1. Предварительный анализ объекта.
			2. Объединение критичных ресурсов в отказоустойчивый кластер.
			3. Тестирование критического сегмента РИС.



Рис. 1 Группы стандартов, содержащих возможные требования профиля критического сегмента распределённой информационной системы



Рис.2. Диаграмма этапов выполнения методики самовосстановления

критического сегмента распределенной информационной системы

**Заключение**

Разработанная в рамках работы студенческой научно-учебной группы кафедры КИС «Проектирование информационных систем» под руководством автора статьи методика предполагает использование технологии кластеров высокой надёжности. Реализацию этапов методики замедляет малое сопровождение стандартами реализации специфичных с точки зрения критичности сегментов. В реализации работы методики должно быть документирование и архивирование всех инцидентов, сбоев, ошибок, что позволит оперативно просматривать историю, включая причины отказа, формировать отчёты и перенаправлять информацию. Как это оформить, чтобы это стало доступно за пределами предприятий, например, внутри отрасли между специалистами по КИИ, также пока не регламентировано стандартами.

Список литературы

1. ГОСТ 27.002-2015 Надежность в технике (ССНТ). Термины и определения [Электронный ресурс]. — Режим доступа: <http://docs.cntd.ru/document/1200136419> (дата обращения: 12.02.19).

2. ГОСТ 24402-88 Телеобработка данных и вычислительные сети. Термины и определения [Электронный ресурс]. — Режим доступа: <http://docs.cntd.ru/document/1200015767> (дата обращения: 12.02.19).

3. ГОСТ Р 55062-2012 Информационные технологии. Системы промышленной автоматизации и их интеграция. Интероперабельность. Основные положения [Электронный ресурс]. — Режим доступа: <http://docs.cntd.ru/document/1200102958> (дата обращения: 12.02.19).

4. ГОСТ 34.003-90 Информационная технология (ИТ). Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения [Электронный ресурс]. — Режим доступа: <http://docs.cntd.ru/document/1200006979> (дата обращения: 12.02.19).

5. ГОСТ 34.602-89 Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы [Электронный ресурс]. — Режим доступа: http://docs.cntd.ru/document/gost-34-602-89 (дата обращения: 12.02.19).

6. ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения [Электронный ресурс]. — Режим доступа: http://docs.cntd.ru/document/1200075565 (дата обращения: 11.02.19).

7. Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 N 187-ФЗ [Электронный ресурс]. — Режим доступа: <http://docs.cntd.ru/document/436752114> (дата обращения: 11.02.19).

8. Носырева Е.В. Применение теории комплексных сетей для выявления критически важных объектов энергетики // Вестник Иркутского государственного технического университета №7, 2017 г. – 52 с.

9. Кононов А.А. Ключевые проблемы обеспечения безопасности Национальной информационной инфраструктуры / Кононов А.А., Черешкин Д.С. // Информационное общество №1, 2012 г. – 8 с

10. ГОСТ 34.321-96 Информационные технологии. Система стандартов по базам данных. Эталонная модель управления данными [Электронный ресурс]. — Режим доступа: http://docs.cntd.ru/document/1200017662 (дата обращения: 12.02.19).

11. Методика отнесения объектов государственной и негосударственной собственности к критически важным объектам для национальной безопасности Российской Федерации. - М.:2012. с 5.

References

1.GOST 27.002-2015 Reliability in engineering (SSNT). Terms and definitions [Electronic resource]. — Mode of access: http://docs.cntd.ru/document/1200136419 (date accessed: 12.02.19).

2. GOST 24402-88 Teleoperate data and computing network. Terms and definitions [Electronic resource]. — Mode of access: http://docs.cntd.ru/document/1200015767 (date accessed: 12.02.19).

3. GOST R 55062-2012 Information technologies. Industrial automation systems and their integration. Interoperability. Main provisions [Electronic resource]. — Mode of access: http://docs.cntd.ru/document/1200102958 (date accessed: 12.02.19).

4. GOST 34.003-90 Information technology (it). A set of standards for automated systems. Automated system. Terms and definitions [Electronic resource]. — Mode of access: http://docs.cntd.ru/document/1200006979 (date accessed: 12.02.19).

5. GOST 34.602-89 Information technology. A set of standards for automated systems. Terms of reference for the creation of an automated system [Electronic resource]. — Mode of access: http://docs.cntd.ru/document/gost-34-602-89 (date accessed: 12.02.19).

6. GOST R 53114-2008. Information security in the organization. Basic terms and definitions [Electronic resource]. — Mode of access: http://docs.cntd.ru/document/1200075565 (date accessed: 11.02.19).

7. Federal law" on security of critical information infrastructure of the Russian Federation " dated 26.07.2017 N 187-FZ [Electronic resource]. — Mode of access: http://docs.cntd.ru/document/436752114 (date accessed: 11.02.19).

8. Nosyreva E. V. application of the theory of complex networks to identify critical facilities energy // Vestnik of Irkutsk state technical University, №7, 2017, 52 p.

9.Key problems of ensuring the security of the National information infrastructure / Kononov, A. A., Chereshkin, D. S. / / Information society ,No. 1, 2012.

10. GOST 34.321-96 Information technologies. System of database standards. Reference model of data management [Electronic resource]. — Mode of access: http://docs.cntd.ru/document/1200017662 (date accessed: 12.02.19).

11. Methods of classifying objects of state and non-state ownership as critical objects for the national security of the Russian Federation. - Moscow: 2012. p.5.