УДК 004.056.53
DOI 10.33764/2618-981X-2022-6-47-53

Вопросы формирования организационно-функциональной структуры системы управления информационной безопасностью значимого объекта критической информационной инфраструктуры

И. Е. Дорошенко[1], М. О. Максудов[1], В. В. Селифанов[1]*

[1] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
* e-mail: Vaas2202@gmail.com

Аннотация. В эпоху лавинообразного развития информационных технологий и их моментального внедрения во все сферы жизни человека остро встает вопрос обеспечения безопасности данных систем. Для организаций чьи активы разбросаны по всей территории РФ, а также за рубежом, встает острая необходимость обеспечения эффективного управления информационной безопасностью в виду большого количества информационных активов, а так же средств защиты, зачастую несогласованных или плохо согласованных между собой. Для решения поставленной задачи в рамках этой работы была разработана модель реализации организационно- функциональной структуры системы управления информационной безопасностью для значимых объектов критической информационной инфраструктуры. Данная модель не является финальной точкой, необходимо провести работу над разработкой нескольких возможных вариантов построения системы, а также оценить эффективность полученных результатов.

Ключевые слова: КИИ, автоматизированная система, система управления безопасностью

Issues of formation of the organizational and functional structure of the information security management system of a significant object of critical information infrastructure

I. E. Doroshenk[1], M. O. Maksudov[1], V. V. Selifanov[1]*

[1] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
* e-mail: Vaas2202@gmail.com

Abstract. In the era of avalanche-like development of information technologies and their instant introduction into all spheres of human life, the issue of ensuring the security of these systems is acute. For organizations whose assets are scattered throughout the territory of the Russian Federation, as well as abroad, there is an urgent need to ensure effective information security management, in view of the large number of information assets, as well as means of protection, often inconsistent or poorly coordinated with each other. To solve this task, within the framework of this work, a model was developed for the implementation of the organizational and functional structure of the information security management system for significant CII facilities. This model is not the final point, it is necessary to work on the development of several possible options for building the system, as well as to evaluate the effectiveness of the results obtained.

Keywords: CII, automated system, security management system

Введение

В эпоху развития информационных технологий происходит не только их молниеносное развитие, но и практически моментальное внедрение во все сферы жизнедеятельности в том числе в сферу государственного управления. Помимо

сферы государственного управления информационные технологии прочно укрепились в производственной среде, на критических предприятиях промышленности государства, а также в финансовом секторе. Так же это именуется как «четвертая промышленная революция» [1].

В сложившейся ситуации: недружественной политики ведущих технологических держав, в том числе введенными санкциями и ограничениями – для обеспечения лидерства России в информационной и технологической сфере к 2035 году была разработана программа «технологическая инициатива» [2], в рамках которой одобрено 8 «дорожных карт» в которые вошли следующие программы: Аэронет, Автонет, Маринет, Нейронет, Хелснет, Энерджинет, Технет и Кружковому движению, около 500 проектов получили финансирование. Ключевыми технологиями в данном направлении были определены следующие:

- большие данные;
- искусственный интеллект;
- системы распределенного реестра;
- квантовые технологии;
- новые и портативные источники энергии;
- новые производственные технологии;
- сенсорика и компоненты робототехники;
- технологии беспроводной связи;
- технологии управления свойствами биологических объектов;
- нейротехнологии и технологии виртуальной и дополненной реальности.

Все это обуславливает появление и актуализацию новых угроз, из этого вытекает необходимость переоценки подходов к обеспечению безопасности информационных систем, а также к управлению системами безопасности информационных систем. Так же целью является обеспечение суверенитета и самостоятельности России в области информационных технологий. Данные положения нашли отражение в Стратегии развития информационного общества в Российской Федерации на 2017 – 2030 годы [3] и в Доктрине информационной безопасности Российской Федерации [14]. Где особое внимание уделяется обеспечению информационной безопасности субъектов и находящихся в их владении объектов критической информационной инфраструктуры (КИИ).

Подход к процессу разработки системы обеспечения кибербезопасности б объектов КИИ или киберзащиты в общем виде возможно представить в виде алгоритма – последовательности выполнения последовательности шагов [5-7]: категорирование (классификация); идентификация и классификация критических активов; предъявление требований и выбор мер для обеспечения защиты и управления доступом, которые определяют будущую архитектуру кибербезопасности системы; разработка и внедрение систем защиты, в том числе организационно-распорядительных документов (ОРД) регламентирующих политики и процедуры безопасности; эксплуатация (управление) системы.

В связи с укрепляющимися тенденциями возможные варианты алгоритмов управления реализованы лишь в виде частично формализованных содержатель-

ных рассуждений на основе интуиции исследователей, рассматривавших этот вопрос [10-13]. Процесс управления является заданным, однако цель создания вариантов организационно-функциональной структуры не решается [6].

С целью решения данной задачи требуется разработать алгоритм синтеза организационно-функциональной структуры системы управления, а также оценить эффективность разработанного алгоритма [6].

Методы и материалы

Система безопасности объектов КИИ является сложной и многоуровневой. Включает в себя совокупность средств и систем защиты информации используемых соответствующими органами и структурами организации, функционирующие по регламентированным для них требованиями и процедурами. Система реализует в соответствии с 27 группами мер, каждая из которых содержит функции автоматизированного управления [9].

В состав системы безопасности включены разные силы и средства, которые распределены на большой территории (от уровня субъектов федерации до федерального уровня), также системы должны быть связаны с государственной системой обнаружения и предупреждения вторжений на информационные ресурсы Российской Федерации, для которых обеспечивается централизованное или децентрализованное управление ими, а также с целью оперативного распределения данных сил и средств в случае возникновения инцидентов безопасности. Состав и структура функций системы должны изменятся в соответствии с возникшими потребностями.

В связи с образовавшимися в данное время тенденциями, возможные варианты алгоритмов управления реализованы лишь в виде частично формализованных содержательных рассуждений на основе интуиции исследователей рассматривавших этот вопрос [11]. Процесс управления является заданным, однако цель создания вариантов организационно-функциональной структуры не решается [8].

С целю решения данной задачи требуется разработать алгоритм синтеза организационно-функциональной структуры системы управления, а также оценить эффективность разработанного алгоритма [9,10].

В рамках решения и достижения поставленной цели рассмотрены не только средства защиты информации, а также все элементы объекта КИИ реализующие функции безопасности. Схематичное представление элементов, реализующих функции безопасности представлено на рис.1.

Под организационно-функциональной структурой автоматизированной системы управления безопасностью понимается совокупность центров управления, связанных между собой посредством подчинения, с соответствующими каждому пункту управления функциями средств безопасности с учетом связи между ними.

Для выполнения работ по разработке одного из вариантов алгоритма построения организационно-функциональной структуры системы управления выбрана система представления на рис.2.

Рис. 1. Схематичное представление элементов, реализующих функции безопасности

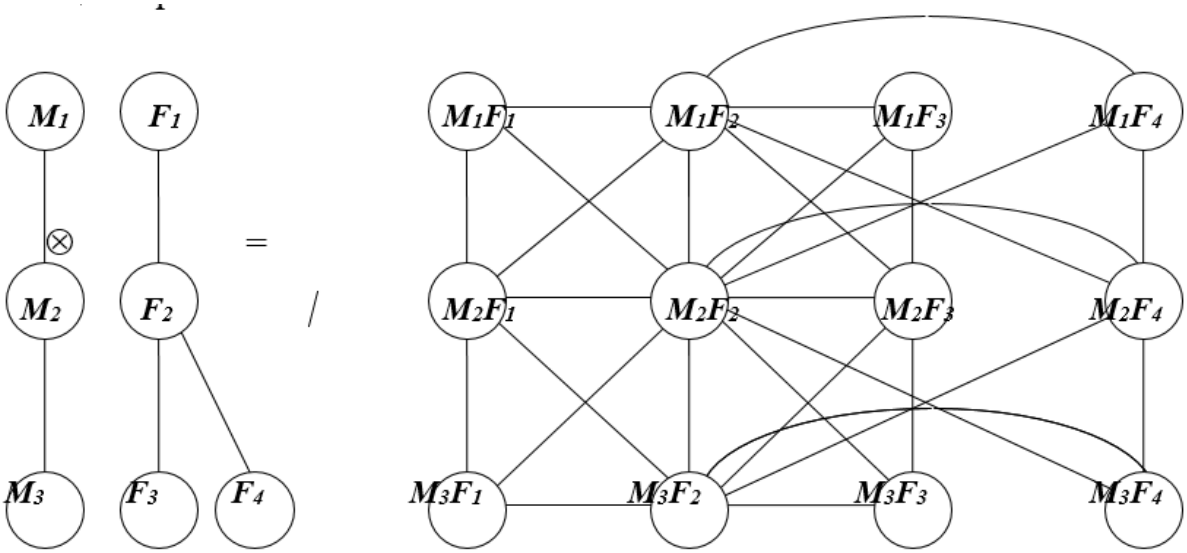

Рис. 2. Пример выполнения операции композиции графов

Для выполнения работ по разработке одного из вариантов алгоритма построения организационно-функциональной структуры системы управления выбрана система, представления на рис. 3.

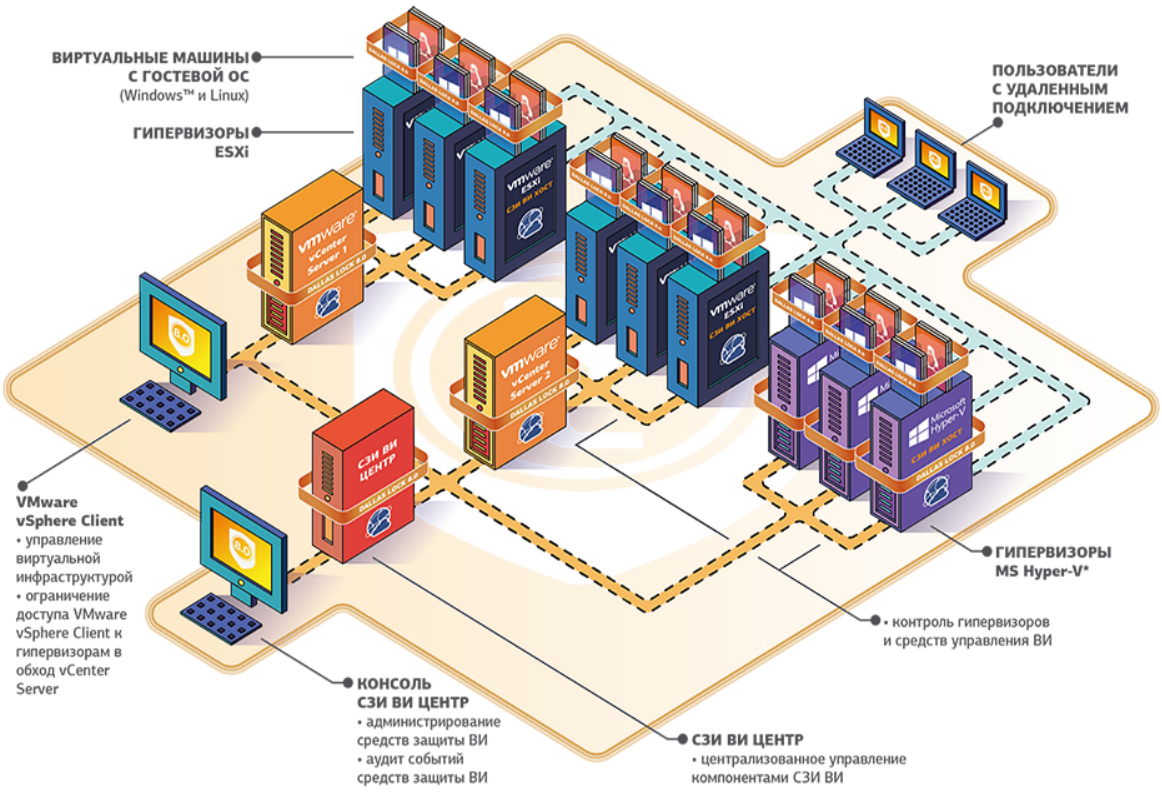

Рис. 3. Базовый пример системы

Результаты

В результате проведенных работ разработан вариант алгоритма создания организационно-функциональной структуры системы управления безопасностью значимого объекта критической информационной инфраструктуры (ЗО КИИ). Последовательность действий при построении допустимых вариантов организационно-функциональной структуры автоматизированной системы безопасности будет следующей.

Шаг 1. Строится матрица смежности для очередного варианта графа допустимого организационного состава и структуры.

Шаг 2. Строится матрица смежности для графа структуры функций автоматизированной системы управления.

Шаг 3. По матрицам смежности рассматриваемого допустимого варианта организационного состава и структуры и структуры функций, а также с учетом ограничений строится и запоминается матрица смежности полного графа всех допустимых вариантов организационно-функциональной структуры.

Шаг 4. Из полного графа всех допустимых вариантов организационно-функциональной структуры выделяется граф отдельного допустимого варианта организационно-функциональной структуры.

Шаг 5. Проверяется, все ли допустимые варианты организационно-функциональной структуры построены для очередного варианта организационного состава и структуры. Если не все, то переход на шаг 4.

Шаг 6. Проверяется, все ли варианты организационного состава и структуры рассмотрены. Если не все, то переход на шаг 1.

Шаг 7. Строятся графы допустимых вариантов организационно-функциональной структуры по полученным матрицам смежности.

Заключение

В ходе выполнения данной работы был разработан один из возможных вариантов алгоритма формирования организационно-функциональной структуры системы управления безопасностью ЗО КИИ. Полученный алгоритм апробирован на тестовой системе: для нее был построен граф допустимых вариантов организационно-функциональной структуры системы управления безопасностью. Полученный граф организационно-функциональной структуры представлен на рис. 4.

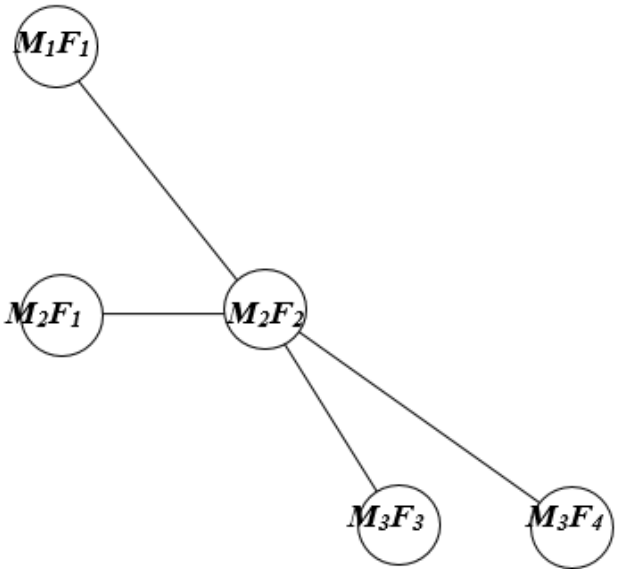

Рис. 4. Результирующий граф организационно-функциональной структуры

Используя полученные результаты будут использованы для разработки других методик формирования структуры систем управления. Для оценки перспектив применения данных методик будет проведена оценка эффективности разработанных методик. После разработки нескольких вариантов формирования организационно-функциональной структуры будет проведена оценка эффективности в соответствии с методикой, описанной в «Построении адаптивной трехуровневой модели процессов управления системой защиты информации объектов критической информационной инфраструктуры» [2].

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Гаджиева Н.А, Гаджиев А.М. Системы управления информационной безопасности предприятия// Сборник материалов 42 итоговой научно-технической конференции преподавателей, сотрудников, аспирантов и студентов ДГТУ. Махачкала, 2021. – С. 394 – 396.

2. Голдобина А.С., Ю.А. Исаева Выбор имитационной модели процессов управления защитой информации для оценки эффективности государственных и муниципальных систем/

Инновационное развитие науки и образования. Сборник статей Международной научно-практической конференции. В 2 частях. Пенза, 2018. – С. 86 – 89.

3. Калашникова А.О, Кульбы В.В., Проблемы управления безопасностью сложных систем // материалы XXVI Междунар. Конфер., Москва / под общ. ред.. – М. : ИПУ РАН. – 2018. – С. 411 – 413.

4. Корниенко А.А., Глухов А.П., Диасамидзе С.В., Глухарев М.Л.,Бирюков Д.Н., Концептуальная модель интеллектуальной системы риск-ориентированного упреждающего управления информационной безопасностью железнодорожного транспорта // Известия петербургского университета путей сообщения Том 15, 2018. – С. 159 – 161.

5. Минзов С.А., Управление событиями информационной безопасности в siem-системах // Материалы двадцать шестой международной научно-технической конференции студентов и аспирантов "радиоэлектроника, электротехника и энергетика", 2020. – С. 299 – 302.

6. Федеральная служба по техническому и экспортному контролю: Приказ ФСТЭК России от 25.12.2017 №239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» – Текст: электронный// Справочная правовая система КонсультантПлюс. – Режим доступа: по подписке (дата обращения 29.04.2022).

7. Федеральный закон от 26.07.2017 № 187 «О безопасности критической информационной инфраструктуры Российской Федерации». // Собрание законодательства Российской Федерации №31, 2017.

8. Дэвис Н., Шваб К., Технологии четвертой промышленной революции. М: Эксмо, 2018 – С. 19 – 22.

9. Губко М.В. Управление организационными системами с коалиционным взаимодействием участников //ИПУ РАН Москва., 2003. – С. 224 – 230.

10. Губко М.В. Математические модели оптимизации иерархических структур // Ленанд, Санкт – Петербург 2006. – С. 230 – 235.

11. Новиков Д.А. Сетевые структуры и организационные системы // ИПУ РАН, Москва. 2003. – С. 198 – 201.

12. Воронин А.А., Мишин С.П. Оптимальные иерархические структуры // ИПУ РАН, Москва. 2003. – С. 250 – 252.

13. Новиков Д.А. Кибернетика: Навигатор. История кибернетики, современное состояние, перспективы развития // Ленанд, Санкт – Петербург 2006. – С. 227 – 229.

14. Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» – Текст: электронный// Справочная правовая система КонсультантПлюс. – Режим доступа: по подписке.