УДК 004.056.53
DOI 10.33764/2618-981X-2022-6-143-148

Проблемы формирования структуры функций системы управления информационной безопасностью значимого объекта критической информационной инфраструктуры

М. О. Максудов[1]*, *И. Е. Дорошенко*[1], *В. В. Селифанов*[1]
[1] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
* e-mail: midat99@mail.ru

Аннотация. В столь напряженной геополитической обстановке, и как следствие, ужесточением законодательства Российской Федерации относительно требований к системам защиты информации объектов критической информационной инфраструктуры, особенно важным становится обеспечение безопасности соответствующих информационных систем. С каждым годом требования к системе защиты информации значимых объектов критической информационной инфраструктуры становятся все серьезнее. Использование множества разнородных средств защиты информации создает противоречие, которое заключается в наличии таковых средств защиты информации и невозможности управления ими централизовано. Таковое противоречие возможно решить, разработав систему управления информационной безопасностью с сформированной структурой функций системы. В данной статье представлен принцип решения задачи формирования структуры функций системы управления информационной безопасностью значимого объекта критической информационной инфраструктуры, приведен принцип построения системы управления информационной безопасностью значимого объекта критической информационной инфраструктуры, а также метод проверки эффективности системы.

Ключевые слова: информационная безопасность, управление безопасностью, критическая информационная инфраструктура

Problems of forming the structure of functions of the information security management system of a significant object of critical information infrastructure

M. O Maksudov[1]*, *I. E. Doroshenko*[1], *V. V. Selifanov*[1]
[1] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
* e-mail: midat99@mail.ru

Abstract. In such a tense geopolitical situation, and as a result, the tightening of the legislation of the Russian Federation regarding the requirements for information protection systems for critical information infrastructure objects, it becomes especially important to ensure the security of critical information infrastructure. Every year, the requirements for the information security system of significant objects of critical information infrastructure become more and more serious. The use of heterogeneous information security tools creates a contradiction, which consists in the presence of such information security tools and the impossibility of their centralized management. Such a contradiction can be resolved by developing an information security management system with a formed structure of the functions of such a system. This article presents the concept of solving the problem of forming the structure of the functions of the information security management system of a significant object of critical information infrastructure, the concept of building an information security management system of a significant object of critical information infrastructure, as well as the concept of checking the effectiveness of such a system.

Keywords: information security, security management, critical information infrastructure

Введение

Вступив в силу, Федеральный закон № 187 «О безопасности критической информационной инфраструктуры Российской Федерации», ввел термины: объект критической информационной инфраструктуры (далее ОКИИ), а также значимый объект критической информационной инфраструктуры (далее ЗО КИИ), а внушительное количество законодательных актов в отношении безопасности критической информационной инфраструктуры определили вектор развития систем защиты информации ЗО КИИ [1,2].

Однако автоматизированная система управления информационной безопасностью не может быть построена без сформированной структуры функций системы управления информационной безопасностью. В связи с чем, целью исследования является анализ возможности разработки методики формирования структуры функций системы управления защитой информации, применимой для ЗО КИИ Российской Федерации.

Для формирования структуры функций системы управления информационной безопасностью ЗО КИИ Российской Федерации, а также последующего построения системы управления информационной безопасностью необходимо:

− проанализировать существующие подходы формирования структуры функций автоматизированной системы управления информационной безопасностью;

− разработать методику формирования структуры функций автоматизированной системы управления информационной безопасности;

− провести моделирование процесса реализации разработанной методики для нескольких ЗО КИИ Российской Федерации;

− оценить эффективность разработанной методики.

На данный момент актуальными являются следующие методы организации систем управления информационной безопасностью:

– построение системы управления информационной безопасности на основе построения модели надежности системы управления информационной безопасностью;

– построение риск-ориентированной системы управления информационной безопасности [3];

– построение классической системы управления информационной безопасностью на основе систем менеджмента инцидентов информационной безопасностью [4].

Однако данные подходы не решают проблемы невозможности автоматизированного управления разнородными средствами защиты информации. В первом и во втором случае, с использованием «модели надежности», или «рискоориентированности» избегаются риски, связанные с полной автоматизацией системы управления информационной безопасности, а также не решается проблема управления разнородными средствами защиты информации [5,6]. В последнем случае системы менеджмента информационной безопасности решают задачи от-

слеживания сигналов и аномалий, а также информирование оператора о возможных инцидентах информационной безопасности, но рассматриваемая система не является полноценной системой управления информационной безопасностью.

Методы и материалы

При отсутствии автоматизации процессом управления информационной безопасностью ЗО КИИ Российской Федерации основной задачей становится реализация процесса формирования структуры функций создаваемой автоматизированной системы управления информационной безопасностью. В таком случае возникает необходимость в разработке методики, которая будет заключаться в составлении модели задач системы защиты информации, что в последствии будет возлагаться на систему управления информационной безопасностью в процессе эксплуатации. Благодаря методике, система управления информационной безопасностью будет способна определять взаимосвязи между задачами, выявлять возможные совпадения таких задач и в построении на этой основе структуры функций системы управления информационной безопасностью. Структура функций будет построена путем подстановки в соответствии каждой задаче и нескольким совпадающим задачам соответствующих им функций автоматизированной системы управления.

После реализации возникнет необходимость осуществить моделирование процесса реализации методики для нескольких ЗО КИИ Российской Федерации, при этом для выявления недостатков разрабатываемой системы необходимо будет реализовать разные варианты систем управления информационной безопасностью для нескольких ЗО КИИ Российской Федерации. Процесс моделирования систем управления информационной безопасностью ЗО КИИ Российской Федерации будет реализован при помощи программного продукта Anylogic. Будет построено три варианта системы управления информационной безопасностью [9,10].

Первая модель является классической системой управления информационной безопасностью информационных систем, относящихся к критической информационной инфраструктуре [3, 7]. На рис. 1 представлена классическая схема сети с разделением сети на офисную и технологическую, с сервером управления (scada/dcs), некоторыми программно-логическими контроллерами (ПЛК), а также с реализованной системой защиты информации, основанной на программно-аппаратном обеспечении лаборатории Касперского [8].

Для управления системой защиты информации (рис. 1) используется операционный центр безопасности (сервер мониторинга с системой менеджмента инцидентов информационной безопасности). Упрощенная схема управления системой защиты представлена рис. 2. Данный вариант все еще имеет ряд недостатков, главным их которых является неполноценность системы управления информационной безопасности.

Второй моделью является рискоориентированная система управления информационной безопасностью ЗО КИИ Российской Федерации, основанная на базе вероятностей тех или иных событий, влекущих инциденты информацион-

ной безопасности или «показателями надежности». Недостаток модели заключается в избегании рисков, связанных с полной автоматизацией системы управления информационной безопасности, а также отсутствии решения проблемы управления разнородными средствами защиты информации [6, 8].

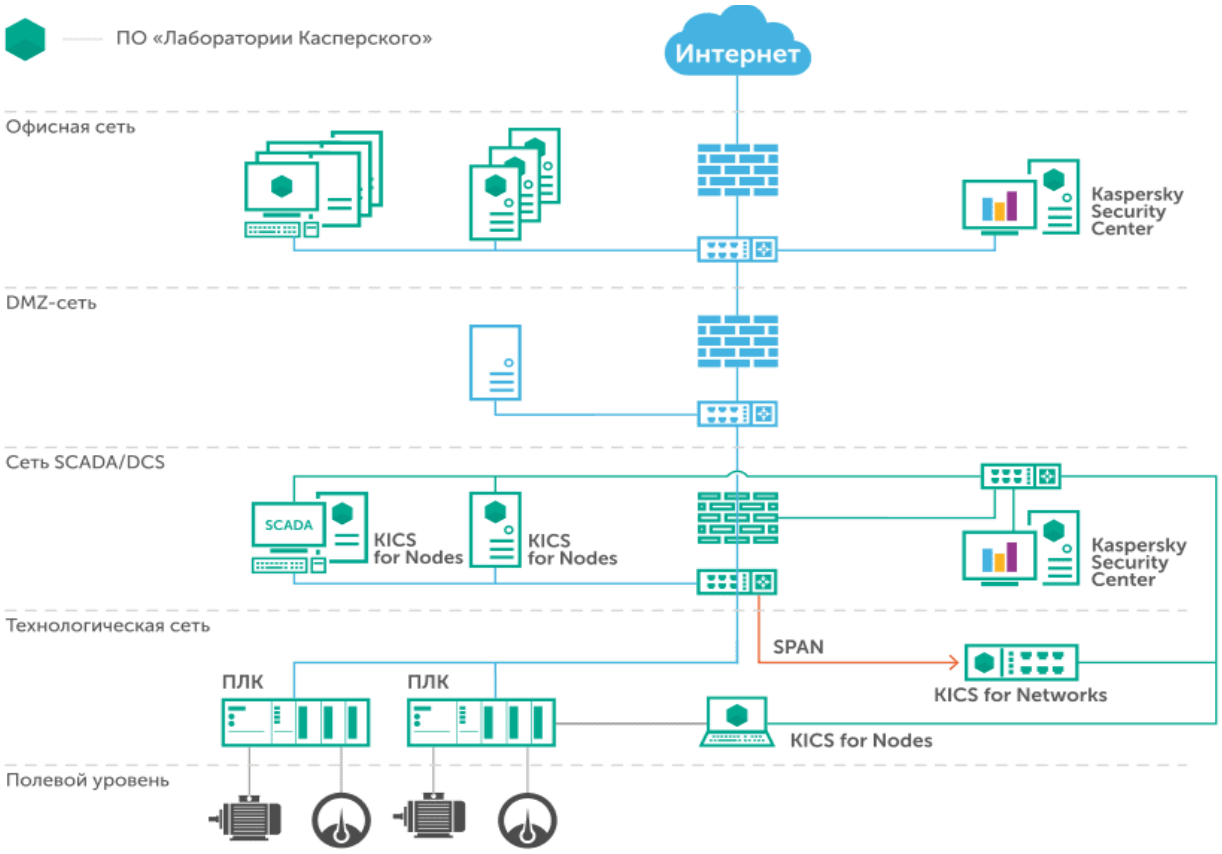

Рис. 1. Классическая схема сети с реализованной системой защиты информации

Рис. 2. Упрощенная схема управления информационной безопасностью

Третья модель системы управления информационной безопасностью строится с использованием разрабатываемой методики формирования структуры функций системы управления информационной безопасности. Ввиду недостатков классического варианта построения системы управления информационной безопасности, а также ее рискоориентированного варианта построения выведены следующие принципы формирования структуры функций системы управления информационной безопасностью:

– осуществляется первоначальная нумерация всех имеющихся задач, возлагаемых на систему защиты информации в соответствии с номерами, их описывающими;

– строится сеть, обеспечивающая определение принадлежности любой задачи к совпадающим задачам;

– вводится описание первой либо очередной задачи;

– последовательно вводятся описания очередных задач системы защиты информации, также совпадающие задачи соответствующе помечаются;

– проверяется, все ли задачи системы защиты информации соотнесены с другими задачами;

– нумерация всех выявленных совокупностей совпадающих задач системы защиты информации.

Результаты

Анализ существующих актуальных вариантов систем управления информационной безопасностью ЗО КИИ Российской Федерации выявил основные недостатки существующих систем управления информационной безопасностью, а именно: в случае построения «рискоориентированной» системы управления информационной безопасностью избегаются риски, связанные с полной автоматизацией системы управления информационной безопасностью, а также не решается проблема управления разнородными средствами защиты информации; в случае построения классической системы управления информационной безопасностью решаются задачи отслеживания сигналов и аномалий, а также информирование оператора о возможных инцидентах информационной безопасности, но рассматриваемая система не является полноценной системой управления информационной безопасностью.

Исходя из анализа существующих актуальных вариантов систем управления информационной безопасностью ЗО КИИ Российской Федерации, определены принципы построения методики формирования структуры функций системы управления информационной безопасностью ЗО КИИ Российской Федерации.

Заключение

Таким образом, полученные результаты будут использованы при разработке методики формирования структуры функций системы управления информационной безопасностью ЗО КИИ Российской Федерации, в соответствии с которой станет возможно построение системы управления информационной безопасно-

стью, которая способна решать задачи, на нее возложенные. Проведено сравнение разрабатываемой системы управления информационной безопасностью с используемыми в данный момент и оценена их эффективность в соответствии с методикой построения адаптивной трехуровневой модели процессов управления системой защиты информации объектов критической информационной инфраструктуры [3].

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. 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).

2. Федеральный закон от 26.07.2017 № 187 «О безопасности критической информационной инфраструктуры Российской Федерации». Текст: непосредственный // Собрание законодательства Российской Федерации №31, 2017. – С. 4736-4789.

3. Голдобина А.С., Исаева Ю.А. 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.

4. Минзов С.А., Управление событиями информационной безопасности в siem-системах – Текст: непосредственный // Материалы двадцать шестой международной научно-технической конференции студентов и аспирантов "радиоэлектроника, электротехника и энергетика", 2020. – С. 299-305.

5. Калашникова А.О, Кульбы В.В., Проблемы управления безопасностью сложных систем – Текст: непосредственный // материалы XXVI Междунар. Конфер., Москва / под общ. ред.. – М. : ИПУ РАН. – 2018. – С. 411-418.

6. 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 – Текст: непосредственный // Известия петербургского университета путей сообщения Том 15, 2018. – С. 152-160.

7. Гаджиева Н.А, Гаджиев А.М. Системы управления информационной безопасности предприятия – Текст: непосредственный // Сборник материалов 42 итоговой научно-технической конференции преподавателей, сотрудников, аспирантов и студентов ДГТУ. Махачкала, 2021. – С. 394-398.

8. Чашкин В. Н. Управление информационной безопасностью как элемент системы управления информационно-технологической деятельностью организации – Текст: непосредственный // Сборник трибуны молодых ученых, Национальный исследовательский ядерный университет МИФИ Том 16, 2009. – С. 123-124.

9. Ан В.Р., Селифанов В.В., Табакаева В.А., Буларга С.А., Ворожцов А.С. Разработка методики аудита кибербезопасности ГИС, относящихся к объектам критической информационной инфраструктуры российской федерации – Текст: непосредственный // Сборник трудов Новосибирского государственного технического университета, 2019. С. 84-95.

10. Табакаева В.А., Селифанов В.В., Ан В.Р., Буларга С.А., Ворожцов А.С. Интеллектуальные системы управления информационной безопасностью – Текст: непосредственный // Сборник трудов Новосибирского государственного технического университета, 2019. С. 165-176.