УДК 004.054.53
DOI: 10.33764/2618-981X-2020-6-2-99-104

ОСОБЕННОСТИ ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Валерия Александровна Табакаева
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, магистрант кафедры фотоники и приборостроения, тел. (962)831-22-52, e-mail: tabakaeva1997@mail.ru

Игорь Николаевич Карманов
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, кандидат технических наук, доцент, зав. кафедрой физики, тел. (903)937-24-90, e-mail: i.n.karmanov@ssga.ru

Владимир Робертович Ан
Новосибирский государственный технический университет, 630073, Россия, г. Новосибирск, пр. Карла Маркса, 20, магистрант кафедры вычислительной техники, тел. (903)939-53-58, e-mail: vovan2011nsk@mail.ru

В данной статье рассматривается проблема использования интеллектуальных систем в управлении информационной безопасностью объектов критической информационной инфраструктуры. В настоящее время процесс развития информационных технологий достиг точки перехода на повсеместное использование различных интеллектуальных систем. При этом отмечается их применение и в сфере обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации. Системы управления параметрами кибербезопасности занимают особое место, как основополагающие элементы для обеспечения безопасности в ходе эксплуатации, и реагирования на внешние и внутренние инциденты с требуемой эффективностью и скоростью. В ходе проводимого исследования выбираются пути решения таких задач, как выбор модели угроз и архитектуры системы защиты объекта критической информационной инфраструктуры Российской Федерации.

Ключевые слова: интеллектуальные системы, информационная безопасность, кибербезопасность, значимый объект, критическая информационная инфраструктура, параметры информационной безопасности, имитационное моделирование.

FEATURES OF INTELLIGENT INFORMATION SECURITY MANAGEMENT SYSTEMS FOR CRITICAL INFORMATION INFRASTRUCTURE OBJECTS

Valeria A. Tabakaeva
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Graduate, Department of Photonics and Device Engineering, phone: (962)831-22-52, e-mail: tabakaeva1997@mail.ru

Igor N. Karmanov
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Ph. D., Associate Professor, Head of the Department of Physics, phone: (903)937-24-90, e-mail: i.n.karmanov@ssga.ru

Vladimir R. An
Novosibirsk State Technical University, 20, K. Marx Prospekt, Novosibirsk, 630073, Russia, Graduate, Department of Computer Science, phone: (903)939-53-58, e-mail: vovan2011nsk@mail.ru

The article discusses the problem of using intelligent systems in managing information security of critical information infrastructure objects. Currently, the development of information technologies reached the point of transition to widespread use of various intelligent systems. At the same time, their application is also noted in the sphere of ensuring the security of significant objects of critical information infrastructure of the Russian Federation. Cybersecurity parameter management systems have a special place as fundamental elements for ensuring security during operation, as well as responding to external and internal incidents with the required efficiency and speed. In the course of the research, we select ways to solve such problems as choosing a threat model and protection system architecture for an object of critical information infrastructure of the Russian Federation.

Key words: intelligent systems, information security, cybersecurity, significant object, critical information infrastructure, information security parameters, simulation.

Введение

Текущий уровень и дальнейшие перспективы развития критической информационной инфраструктуры (КИИ) Российской Федерации сложно представить без внимания, уделяемого вопросам информационной безопасности (ИБ) и кибербезопасности (КБ). Отчасти это связано с растущим числом киберугроз и разрушительных воздействий на объекты КИИ [1].

Системы информационной безопасности должны обеспечивать непрерывное обслуживание клиентов, реализовывать меры защиты от внешних и внутренних угроз. Достичь нужного результата можно с использованием нескольких средств защиты информации. В одной информационной системе могут быть использованы десятки и даже сотни средств защиты [2].

При этом для работы даже средних по размерам сетей (от 1000 рабочих мест), сил одного подразделения уже не хватает, поскольку надо обработать большое количество событий ИБ, поступающих не только от разных средств защиты, но и от других компонентов инфраструктуры. Допустимое время реакции на цепочки событий в системе становится все меньше, и человеческому коллективу необходимы интеллектуальные помощники [3].

Методы и материалы

Рост числа киберугроз объектов КИИ вызвал всплеск исследований в области разработки систем защиты с использованием интеллектуальных систем [4]. Условно можно выделить две группы интеллектуальных систем: системы, применяемые непосредственно в средствах КБ, и системы, применяемые для обеспечения эксплуатации систем КБ значимых объектов КИИ [5].

В настоящее время основные исследования направлены на использование интеллектуальных систем, как составляющей непосредственно средств кибербезопасности [6], например, таких как системы обнаружения вторжений (СОВ), антивирусы и SIEM-системы. Чаще всего в исследованиях для реализации средств и систем защиты используют искусственные нейронные сети (ИНС) [7].

Для того чтобы успешно обеспечивать защиту объектов КИИ, необходимы не только эффективные средства защиты, но и эффективная система управления защитой информации (СУЗИ). Поскольку объекты контроля, СУЗИ, являются организационно-техническими структурами, которые работают в условиях неопределенности, эффективное управление такими системами должно основываться на инновационных информационных технологиях поддержки принятия решений [8].

Существующие требования в области защиты информации не формируют конкретные подходы к управлению КБ объектов КИИ, и это усложняет процедуры проектирования рабочих программных продуктов, которые позволили бы адекватно оценивать степень защиты [9].

Системы обеспечения безопасности объектов КИИ имеют сложную многоуровневую структуру, представляющую собой совокупность средств защиты информации (ЗИ), используемых подразделениями (органами) ЗИ объектов КИИ, организованную и функционирующую по установленным правилам и нормам, реализующую 27 групп мер, каждая из которых включает в себя функции автоматизированного управления [10].

На данном этапе необходимо рассмотреть требования к будущей модели работы интеллектуальной системы поддержки принятия решений (ИСППР) значимых объектов КИИ, позволяющей выбирать рациональные варианты ответа на события КБ [11].

ИСППР должна иметь следующие характеристики:

– позволять оценить уровень защиты объекта КИИ;

– позволять назначать исходные данные по количеству сегментов и узлов объекта КИИ с учетом уровней критичности;

– обеспечивать эффективность в оценке наборов средств защиты информации (СЗИ);

– позволять проводить сравнительный анализ различных комплексов СЗИ при управлении рисками;

– позволять учитывать специфику функционирования конкретного объекта КИИ и реальные угрозы ключевым ресурсам.

Для этого необходимо решить следующие задачи:

– разработать архитектуру системы управления защитой информации объекта КИИ [12];

– усовершенствовать модели оперативного управления КБ объекта КИИ, что даст возможность повысить эффективность управления ИБ в условиях неопределенности состояния объекта КИИ, а также усовершенствовать процесс планирования рациональной структуры системы ЗИ;

– разработать программный комплекс ИСППР для управления КБ объекта КИИ и исследовать эффективность предложенной модели.

Для построения системы управления информационной безопасностью (СУИБ) необходимо выбрать модель угроз; на основе принципов управления в условиях неопределенности и выбранной модели угроз составить обобщенную архитектуру СУИБ [13].

Например, в [14] выбрана следующая модель угроз:

$$OI = \left\{ \bigcup_{j=1}^{W} B^j, \bigcup_{j=1}^{W} INF^j, \bigcup_{j=1}^{W} RES^j, \bigcup_{j=1}^{W} VUL^j, \bigcup_{j=1}^{W} U^j, \bigcup_{j=1}^{W} COM^j, D_r^j \right\}, \quad (1)$$

где B^J – бизнес-процесс предприятия; INF^j – множество типов информационных массивов; RES^j – ресурсы объекта КИИ; VUL^j – набор уязвимостей объекта КИИ; U^j – набор пользователей объекта КИИ; COM – набор информационных потоков объекта КИИ; D^j_r – множество состояний объекта КИИ; j=1,2,... ,i.

Обобщенная архитектура СУИБ представлена на рис. 1.

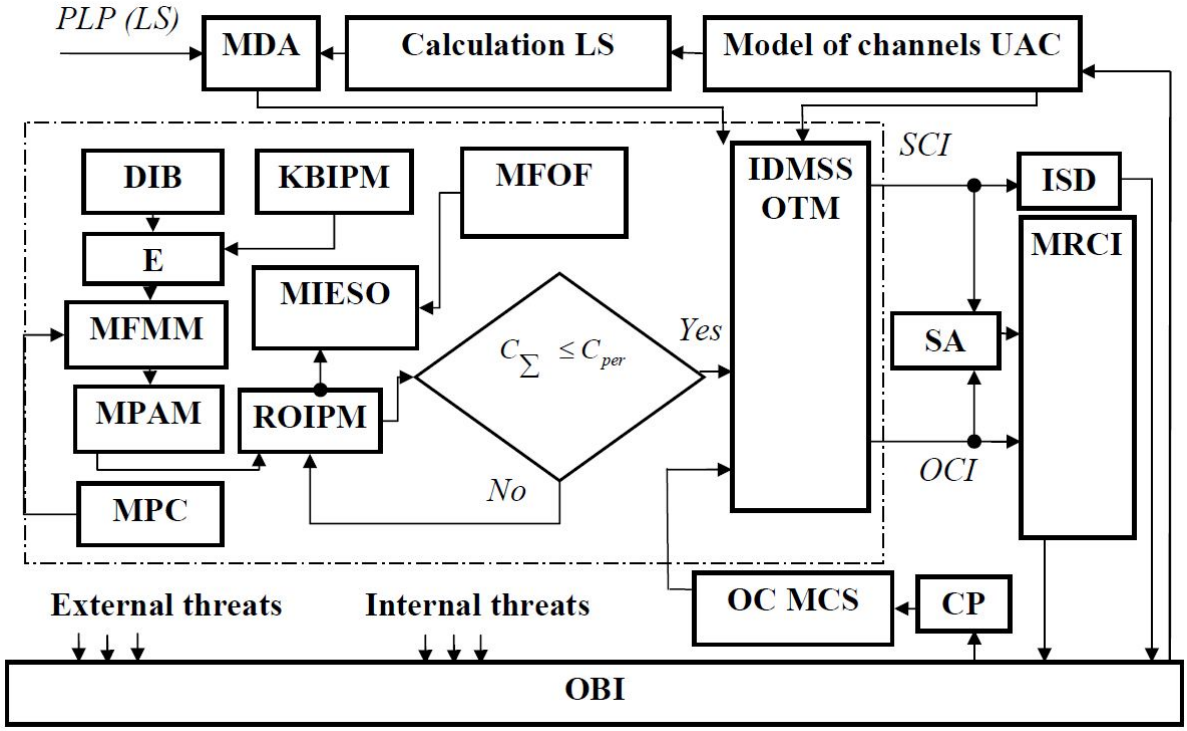

Рис. 1. Обобщенная архитектура СУИБ

Приняты следующие сокращения:

SA – администратор безопасности; DIB – блок ввода данных;

KBIPM – база знаний средств защиты информации;

ISD – отдел информационной безопасности;

E – эксперты;

MRCI – средства реализации управляющих воздействий на управляющие модули, встроенные в IPM;

CP – контролируемые параметры;

MIESO – модуль для осуществления исчерпывающего поиска алгоритм выбора опций из совместимого программного и аппаратного обеспечения средства;

OC MCS – модуль контроля за состоянием объекта контроля;

MDA – модуль оценки отклонений;
MPAM – модуль для обработки дополнительных матриц;
MPC – матрицы попарных сравнений;
MFMM – модуль для формирование морфологических матриц;
MFOF – модуль для формирования целевой функции;
OCI – операционная командная информация;
PLP – первичный уровень защиты;
SCI – плановая командная информация;
ROIPM – рациональные варианты средств защиты информации;
IDMSS – интеллектуальная система поддержки принятия решений по оперативному контролю защиты информации.

Для того, чтобы выявить достоинства и недостатки предложенной модели, необходимо апробировать модель в среде имитационного моделирования AnyLogic.

Заключение

В работе проведен обзор средств и систем защиты информации, выделены две группы интеллектуальных систем, применяемые непосредственно в средствах КБ, и интеллектуальные системы, применяемые для обеспечения эксплуатации систем КБ значимых объектов КИИ. Предложена архитектура системы управления ИБ объекта КИИ.

В дальнейших исследованиях планируется усовершенствовать архитектуру СУИБ, построить модель оперативного управления КБ объекта КИИ и исследовать эффективность предложенной модели.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Taranpreet Kaur, Manvjeet Kaur Cryptographic key generation from multimodal template using fuzzy extractor [Electronic resource]. – Mode of access: https://www.computer.org/csdl/proceedings-article/2017/ic3/12OmNCvLY1P/12OmNBziB93 (дата обращения: 01.03.2020).

2. Сычугов А. А. Обнаружение сетевых атак на основе искусственных иммунных систем [Текст] / А. А.Сычугов, В. Л. Токарев, А. П. Анчишкин. – Тула: Известия ТулГУ, Технические науки №10. 2018. – С. 36-40.

3. Guoli W. Traffic Prediction and Attack Detection Approach Based on PSO Optimized Elman Neural Network // 11th International Conference on Measuring Technology and Mechatronics Automation. Vol. 1. PP. 504-508.

4. Fu Y., et al. An Intelligent Network Attack Detection Method Based on RNN // Data Science in Cyberspace. Vol. 1. PP. 483-489.

5. Hai-He T. Intrusion Detection Method Based on Improved Neural Network \\ International Conference on Smart Grid and Electrical Automation. Vol. 1. PP. 151-154.

6. Daniel Hooks D., Yuan X., Roy K., Esterline A., Hernandez J. Applying Artificial Immune System for Intrusion Detection // in Big Data Computing Service and Applications. Vol.1. PP. 287-292.

7. Ahmad Khalil A., Mbarek N. Togni O. Fuzzy Logic Based Security Trust Evaluation for IoT Environments // 16th International Conference on Computer Systems and Applications. Vol. 1. PP. 1-8.

8. Youakim Badr Y., Banerjee S. Managing End-to-End Security Risks with Fuzzy Logic in Service-Oriented Architectures // in 2013 IEEE World Congress on Services. Vol. PP. 111-117.

9. Tran D., Sharma D., Ma W., Sulaiman R. A Multi-agent Security Architecture // in Network and System Security. Vol. 1. PP. 184-191.

10. Tsochev G. Some Security Model Based on Multi Agent Systems // International Conference on Control, Artificial Intelligence, Robotics & Optimization Vol. 1. PP. 32-36.

11. Селифанов В. В. Построение адаптивной трехуровневой модели процессов управления системой защиты информации объектов критической информационной инфраструктуры [Текст] / В. В Селифанов., А. С.Голдобина, Ю. А.Исаева, А. М.Климова, П. С. Зенкин. – Томск: Доклады Томского государственного университета систем управления и радиоэлектроники., Том 21. № 4. 2018. – С. 51-58.

12. Селифанов, В. В. Методика формирования структуры функций управления защитой информации значимых объектов критической информационной инфраструктуры Российской Федерации [Текст] /В. В. Селифанов. – Омск: Математические структуры и моделирование, № 1(49), 2019. – С 97-106.

13. S. Bellovin. Layered Insecurity // IEEE Security & Privacy. Vol. 17. №. 03. 2019. P. 96–95.

14. V. Lakhno, Y. Boiko Development of the intelligent decision-making support system to manage cyber protection at the object of informatization // Eastern-European Journal of Enterprise Technologies Vol 2, № 9 (86). 2017. P.53-61