УДК 004.054.53
DOI: 10.33764/2618-981X-2021-8-337-343

ПРИМЕНЕНИЕ ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМ В ОПТИЧЕСКИХ СИСТЕМАХ СВЯЗИ ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Валерия Александровна Табакаева
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, магистрант кафедры фотоники и приборостроения, тел. +7 (962) 831-22-52, e-mail: tabakaeva1997@mail.ru

Валентин Валерьевич Селифанов
Новосибирский государственный технический университет, 630073, Россия, г. Новосибирск, пр. Карла Маркса, 20, старший преподаватель кафедры защиты информации, e-mail: sfo1@mail.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

Управление информационной безопасностью в оптических сетях – это актуальная задача, требующая современного подхода, в работе для решения данной проблемы предложено использование интеллектуальных систем. Проведен анализ интеллектуальных систем, выбрана наиболее подходящая интеллектуальная система для решения поставленной задачи.

Ключевые слова: интеллектуальные системы, информационная безопасность, кибербезопасность, антивирусная защита, параметры информационной безопасности

APPLICATION OF INTELLIGENT SYSTEMS IN OPTICAL COMMUNICATION SYSTEMS TO ENSURE INFORMATION SECURITY

Valeria A. Tabakaeva
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Graduate, Department of Photonics and Device Engineering, phone: +7 (962) 831-22-52, e-mail: tabakaeva1997@mail.ru

Valentin. V. Selivanov
Novosibirsk State Technical University, 20, K. Marx Prospekt, Novosibirsk, 630073, Russia, Senior Lecturer, Department of Information Protection, e-mail: sfo1@mail.ru

Vladimir R. An
Novosibirsk State Technical University, 20, K. Marx Prospekt, Novosibirsk, 630073, Russia, Graduate, Department of Computer Science, phone: +7 (903) 939-53-58, e-mail: vovan2011nsk@mail.ru

Information security management in optical networks is an urgent task that requires a modern approach; the use of intelligent systems has been proposed to solve this problem. The analysis of intelligent systems is carried out, the most suitable intelligent system for solving the problem is selected.

Keywords: intelligent systems, information security, cyber security, anti-virus protection, information security parameters

Введение

Одной из главных причин, по которой возникают сложности в управлении параметрами информационной безопасности в информационных системах, является постоянное изменение состояния объектов управления и требований к качеству регулирования в процессе работы. Учитывая, что мы не можем построить аналитическую модель объекта, использование классической теории автоматического управления невозможно. Использование классической теории не дает нужных результатов в условиях неопределенности.

В условиях неопределенности для решения задач управления применяются интеллектуальные системы, их отличительная особенность состоит в одновременном использовании преимуществ классических средств управления и методов искусственного интеллекта. Применение интеллектуальных систем управления – актуальная задача, которая находит широкое применение, в частности, при управлении параметрами информационной безопасности в оптических системах связи.

Необходимость использования интеллектуальных систем

Современный мир невозможно представить без информационных технологий. Самый ценный и востребованный ресурс сегодня – это информация. От того, насколько устойчива к внешним и внутренним угрозам информационная система, зависит непрерывность бизнес-процессов практически любой организации (предприятия, государственного учреждения, учебного заведения, банка и т.д.). Это приводит к появлению большого количества злоумышленников, желающих заполучить конфиденциальную информацию, способных модифицировать известные угрозы безопасности или создавать новые, используя уязвимости нулевого дня, с помощью тех же информационных технологий. Последствиями реализации компьютерных атак могут быть нарушения свойств защищенности информации, таких как конфиденциальность, целостность и доступность. Обладатели информационных систем вынуждены развивать, модифицировать, масштабировать, защищать и адаптировать информационные технологии под текущие условия эксплуатации. По причине того, что замедление или прекращение деятельности объекта в результате успешной кибератаки может привести к социальному, политическому, экономическому или экологическому кризису.

Для исключения возможности появления уязвимостей в системе используются различные средства защиты:

- системы защиты пользователя от нежелательного контента;
- анализ исходного кода;
- межсетевые экраны и системы обнаружения вторжений (IPS);
- контроль привилегированных пользователей (PUM);
- защита АСУ ТП;
- антифрод;
- управление учетными данными (IDM);

– резервное копирование;
– защита от DDoS;
– защита мобильных устройств;
– управление событиями безопасности (SIEM);
– защита веб-приложений (WAF);
– системы обнаружения аномального поведения пользователей (UEBA);
– защита от таргетированных атак;
– защита от утечек данных (DLP);
– шифрование;
– системы отказоустойчивости.

В некоторых случаях при построении комплексной системы защиты необходимо использовать десятки разных средств, учитывать их совместимость, условия эксплуатации информационных систем и их назначение [1].

В этом случае проблема состоит в том, что ответственное лицо должно принимать решения и действовать, учитывая факторы неопределенности, связанные с наличием крайне высокого количества информации и ее неточностью, недостоверностью и несогласованностью с исходными данными.

Попытки управления отдельными средствами защиты в целом являются довольно ограниченными и, в силу указанных выше причин, не позволяют решать поставленные задачи в полном объеме.

Возможный выход из сложившейся ситуации состоит в применении интеллектуальных систем для управления параметрами средств защиты информации.

Для того чтобы построить интеллектуальную систему управления, необходимо проанализировать существующие классы структур систем управления:
– децентрализованную;
– централизованную;
– централизованную рассредоточенную;
– иерархическую.

Децентрализованная структура не подходит для рассматриваемой задачи, так как используется для управления независимыми друг от друга объектами.

Централизованная и централизованная рассредоточенная структуры не могут обеспечить быстрое реагирование на изменение состояния объекта управления, а также при увеличении объема информации возникает сложность синхронизации процессов обмена информацией.

Иерархическая структура является наиболее подходящей для рассматриваемой задачи, так как позволяет выстраивать иерархическую пирамиду управления по мере роста сложности системы.

Принцип работы интеллектуальной системы (ИС)

Интеллектуальная система должна своевременно реагировать на изменения окружающего мира и прогнозировать возможные изменения состояния объекта управления (ОУ).

Прогнозирование изменений состояния ОУ имеет ряд особенностей:

– многообразие исполняемых одновременно процессов и их взаимосвязь, из-за чего нет возможности детально рассмотреть и исследовать каждый процесс – все процессы, происходящие на ОУ необходимо рассматривать в целом;

– отсутствие необходимой количественной информации об изменениях происходящих на ОУ процессов, из-за чего приходится применять качественный анализ таких процессов;

– непостоянность самих процессов, при этом изменения характеристик процессов чаще всего неизвестны, что затрудняет построение их количественных моделей.

Учитывая приведенные выше особенности, ИС будет слабо формализуема, применение традиционных подходов при анализе процессов, происходящих на ОУ для оказания управляющего воздействии не представляется возможным. Появляется необходимость использования методов искусственного интеллекта.

Наиболее подходящим методом прогнозирования для управления информационной безопасностью является когнитивное моделирование (КМ). Цель КМ заключается в генерации и проверке гипотез о функциональной структуре наблюдаемой ситуации до получения функциональной структуры, способной объяснить поведение наблюдаемой ситуации. Применение КМ позволяет определить возможные и рациональные пути управления ситуацией с целью перехода от негативных исходных состояний к позитивным. Данный метод является наиболее подходящим для проектируемой ИС, так как позволяет проводить анализ процессов, следить за состоянием ОУ, прогнозировать возможные состояния ОУ, управлять состоянием ОУ.

Интеллектуальная система управления информационной безопасностью должна иметь как минимум три уровня управления:

– организационный уровень;
– координационный уровень;
– исполнительный уровень.

На организационном уровне происходит сбор, обработка данных, используется когнитивное моделирование, формируются когнитивные карты и модели, после чего моделируется сценарий прогноза событий с выбранным комплексом действий.

На координационном уровне создается база данных, в которую заносятся данные о действиях системы, объектов управления и данные о внешней среде. Происходит анализ принятых данных, проверяется их достоверность при помощи сравнения с уже существующими данными.

На исполнительном уровне происходит определение объектов оказания управляющего воздействия, расстановка очередности оказания управляющего воздействия по степени влияния изменения параметра на состояние объекта управления, создаются команды для оказания управляющего воздействия на объект. Формируется канал для осуществления передачи изменений параметров средств защиты информации.

Для построения модели управления информационной безопасностью в оптических системах связи разработан алгоритм трехуровневого управления, который включает в себя следующие действия:

$^2D_1$ – получение данных об объекте управления (далее – ОУ);

$^2D_2$ – формирование когнитивной карты;

$^2D_3$ – формирование когнитивной модели;

$^2D_4$ – моделирование сценария прогноза событий с выбранным комплексом действий;

$^2D_5$ – прием от вышестоящего пункта управления (ПУ) данных об объектах, назначенных для осуществления воздействия;

$^2D_6$ – формируют базу данных своих действий, объектов воздействия и условий обстановки;

$^2D_7$ – анализ принятых данных на полноту путем их сравнения с ранее введенными в базу данных;

$^2D_8$ – при необходимости, доопределение данных об объектах воздействия;

$^2D_9$ – идентификация объектов воздействия;

$^2D_{10}$ – классификация объектов воздействия;

$^2D_{11}$ – определение приоритетов объектов воздействия;

$^2D_{12}$ – формирование списка объектов воздействия;

$^2D_{13}$ – оценка эффективности осуществления;

$^2D_{14}$ – формирование случайным образом списка действий, значения эффективности которых оказались достаточными для осуществления воздействия на объекты из сформированного списка;

$^2D_{15}$ – формирование целеуказаний для осуществления воздействия на выбранные объекты;

$^2D_{16}$ – формирование команд управления;

$^2D_{17}$ – передача команд управления техническим средствам.

На рис. 1 изображена схема алгоритма трехуровневого управления.

Для того чтобы оценить эффективность предложенной модели управления необходимо построить имитационную модель процессов управления.

Заключение

Управление информационной безопасностью в оптических сетях – это актуальная задача, требующая современного подхода, в работе для решения данной проблемы предложено использование интеллектуальных систем. Проведен анализ интеллектуальных систем, выбрана наиболее подходящая интеллектуальная система для решения поставленной задачи.

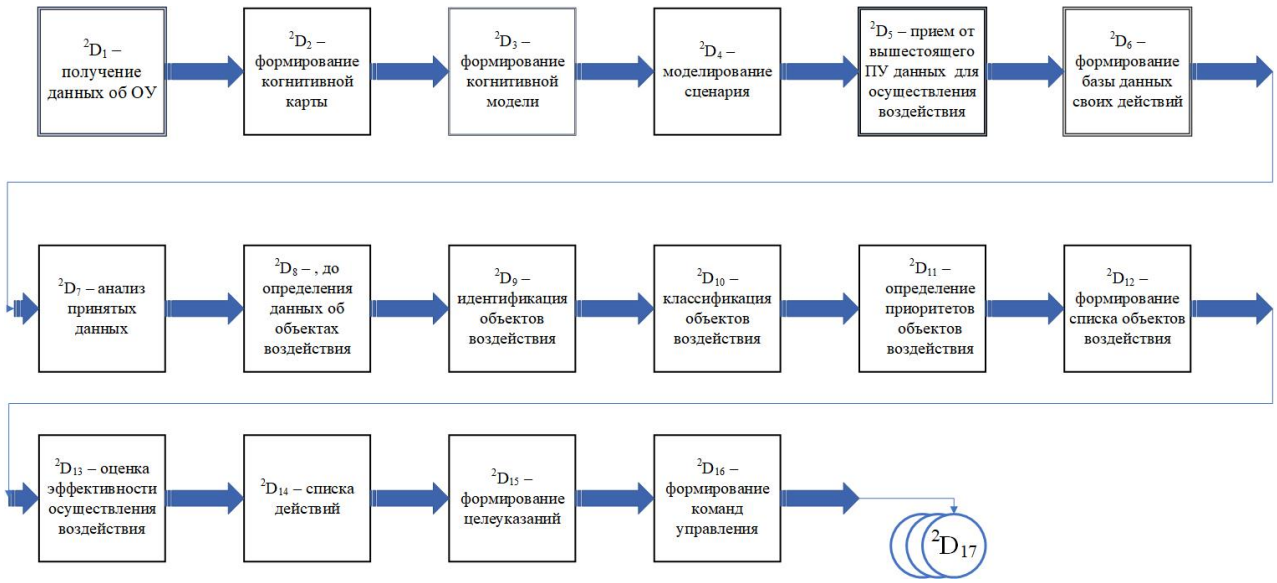

Рис. 1. Алгоритм трехуровневого управления

В дальнейших исследованиях планируется разработать архитектуру интеллектуальной системы управления информационной безопасностью, построить модель оперативного управления информационной безопасностью объекта и исследовать эффективность предложенной модели.

БИБЛИГРАФИЧЕСКЙ 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.

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. 1. – 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.