УДК 004.054.53
DOI: 10.33764/2618-981X-2021-6-281-286

ВЫБОР ПАРАМЕТРОВ УПРАВЛЕНИЯ АНТИВИРУСНОЙ ЗАЩИТОЙ В ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМАХ

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 выбора параметров управления системами антивирусной защиты в интеллектуальных системах. Проведен анализ антивирусных систем, выделены основные функции антивирусных систем, их основные различия, достоинства и недостатки разных подходов. На основе проведённого анализа выбраны параметры управления.

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

SELECTION OF CONTROL PARAMETERS OF ANTI-VIRUS PROTECTION IN INTELLIGENT SYSTEMS

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. Marks Prospekt, Novosibirsk, 630073, Russia, Graduate, Department of Computer Science, phone: (903)939-53-58, e-mail: vovan2011nsk@mail.ru

This article discusses the problem of choosing the settings for managing anti-virus protection systems in intelligent systems. The analysis of antivirus systems is carried out, the main types of antivirus systems are highlighted, their main differences, pros and cons of different approaches. Based on the analysis performed, the control parameters were selected.

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

Введение

Главной причиной, затрудняющей управление системами защиты информации, является существенная девиация как внешнего воздействия, так и состояния защищаемого объекта, что практически исключает возможность использования стандартных методов автоматического управления для построения и эксплуатации современных сложных систем защиты информации [1].

В рассматриваемой ситуации необходимо применение интеллектуальных систем, отличительной особенностью которых является одновременное использование преимуществ стандартных методов управления в совокупности с инструментами искусственного интеллекта.

Для интеллектуальной системы управления необходимо выбрать параметры управления. Из большого количества параметров антивирусных систем необходимо выбрать те, которые подлежат регулированию и изменением которых целесообразно вносить регулирующие воздействия. В данной работе рассмотрим выбор параметров управления системами антивирусной защиты.

Функции антивирусных систем

Можно выделить следующие функции антивирусных систем:

– запуск обновления баз сигнатур;

– изменение областей памяти для сканирования;

– изменение контрольных сумм;

– изменение заданного списка действий подлежащих контролю;

– блокирование опасных действий.

Запуск обновления происходит после анализа интеллектуальной системой (далее – ИС) баз сигнатур, при появлении новых сигнатур запускается обновление.

Изменение областей памяти для сканирования: антивирус проверяет заданные области памяти системы при возникновении связанных с ними событий, например, проверка файла при его копировании или переименовании. Если зараженный файл попадает в другую часть области памяти, в которой мониторинг не происходит, то антивирус не обнаружит угрозу, поэтому необходимо при скачивании новых файлов изменять область сканирования.

Изменение контрольных сумм: при установке нового программного обеспечения (ПО), компонентов ПО и обновлении ПО, изменяются контрольные суммы. Чтобы антивирус не воспринимал эти изменения как нарушение целостности, необходимо изменение контрольных сумм.

Изменение заданного списка действий, подлежащих контролю: антивирус постоянно находится в оперативной памяти и контролирует заданные действия. Если поставить на контроль все действия, которые могут нанести вред системе, то показатели производительности и быстродействия упадут, поэтому необходимо, исходя из состояния системы и происходящих в данный момент процессов, менять список контролируемых действий [10].

Блокирование опасных действий: при обнаружении подозрительной активности происходит блокирование опасных действий.

Принцип работы интеллектуальной системы

Для выбора параметров управления антивирусными системами необходимо учитывать не только функции этих систем, но и принцип работы интеллектуальной системы.

Интеллектуальная система имеет три уровня управления:

– организационный уровень;

– координационный уровень;

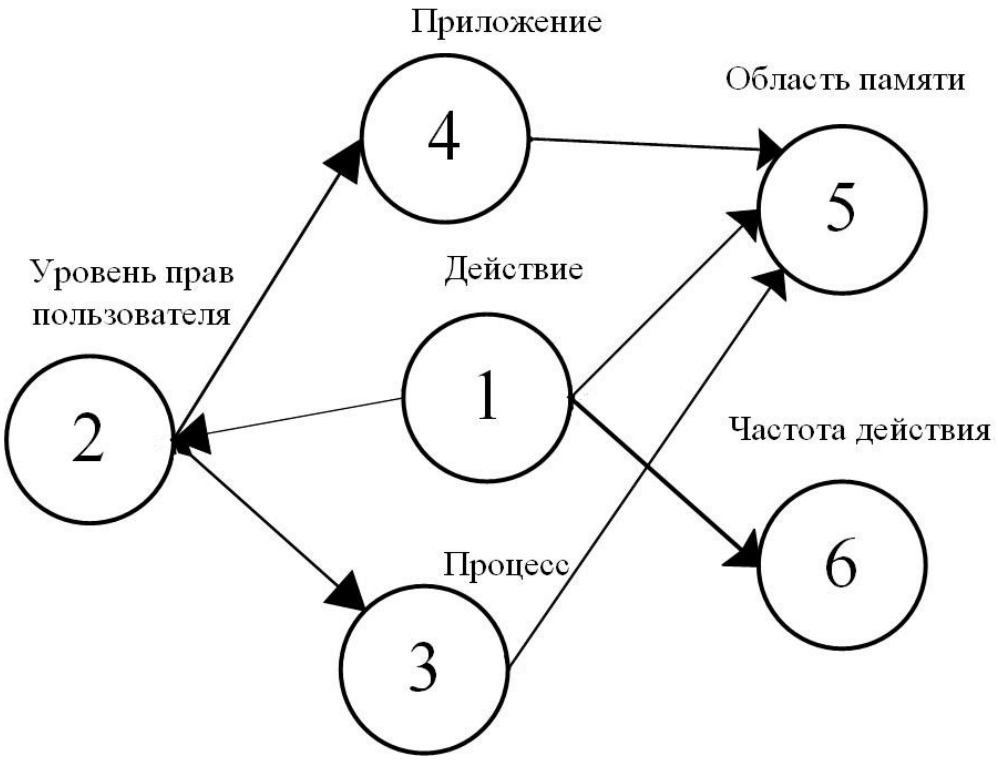
– исполнительный уровень.

На организационном уровне используется когнитивное моделирование, формируются когнитивные карты и модели, после чего моделируется сценарий прогноза событий с выбранным комплексом действий. Формируется база данных действий, объектов воздействия и условий обстановки, анализируются принятые данные на полноту путем их сравнения с ранее введенными в базу данных, при необходимости, доопределения данных об объектах воздействия.

На координационном уровне происходит идентификация объектов воздействия, определение приоритетов объектов воздействия, формирование целеуказаний для осуществления воздействия на выбранные объекты.

На исполнительном уровне формируются команды управления, осуществляется передача команд управления техническим средствам.

Учитывая специфику работы систем антивирусной защиты, разработана когнитивная карта, представленная на рисунке.



Когнитивная карта системы антивирусной защиты

Выбор параметров

Исходя из основных функций антивирусных систем и выбранной модели интеллектуальной системы, были выбраны параметры управления, представленные в таблице.

Параметры управления системой антивирусной защиты

Функция	Параметр	Значения
Изменение областей памяти для сканирования	Сканирование электронной почты	0 или 1
	Проверка подключенных сетевых дисков	0 или 1
	Проверка архивных файлов	0 или 1
	Проверка файлов в сети	0 или 1
	Проверка упакованных исполняемых файлов	0 или 1
	Проверка съемных носителей	0 или 1
	Определение уровня вложенных папок в папке архива для проверки	0 или 1
запуск обновления баз сигнатур	Интервал для распределения запуска обновления	1,2, 3...24 ч.
Изменение контрольных сумм	Изменение контрольных сумм	0 или 1
Изменение заданного списка действий, подлежащих контролю	Контроль запуска приложений	0 или 1
	Контроль запуска инсталляторов	0 или 1
Блокирование опасных действий	Удаление объектов доступа	0 или 1
	Изменения объектов доступа	0 или 1
	Модификация объектов доступа	0 или 1
	Копирование объектов доступа	0 или 1
	Изменение матрицы доступа	0 или 1

В таблице указаны возможные значения параметров, где «1» – это включено, а «0» –выключено. Параметр «Интервал для распределения запуска обновления» измеряется в часах: от 1 обновления в час до 1 обновления за 24 часа.

Заключение

В работе проведен анализ систем антивирусной защиты информации, выделены основные функции систем антивирусной защиты, и на их основе выбраны наиболее эффективные параметры для оказания управляющего воздействия, обеспечивающие наибольшую точность и максимальное качество управления.

Выбранные параметры будут использованы в интеллектуальной системе для управления антивирусной защитой в оптических системах связи. В дальнейших исследованиях планируется построить модель управления информационной безопасностью объекта и исследовать эффективность предложенной модели.

БИБЛИОГРАФИЧЕСКЙ 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. – 2019. – Vol. 1. – PP. 504-508.

4. Fu Y., et al. An Intelligent Network Attack Detection Method Based on RNN // Data Science in Cyberspace. – 2018. – 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. – 2018. –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. – 2018. – 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. – 2019. – Vol. 1. – PP. 1-8.

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

9. Tran D., Sharma D., Ma W., Sulaiman R. A Multi-agent Security Architecture // 2009 Third International Conference on Network and System Security. – 2009. – Vol. 1. PP. 184-191.

10. G. Tsochev, R. Trifonov, R. Yoshinov, S. Manolov, G. Popov and G. Pavlova Some Security Model Based on Multi Agent Systems // International Conference on Control, Artificial Intelligence, Robotics & Optimization. – 2018. – Vol. 1. – PP. 32-36.

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

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

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

14. Lakhno, V., Boiko, Y., Mishchenko, A., Kozlovskii, V. & Pupchenko, O. 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. – No. 9 (86). – 2017. – PP. 53–61.