DOI: 10.18137/RNU.V9187.24.03.P.116 УДК 004.056.52

С.С. Валеев, Н.В. Кондратьева, М.Б. Гузаиров, А.С. Исмагилова

МНОГОАГЕНТНЫЕ СИСТЕМЫ КАК ТЕХНОЛОГИЧЕСКАЯ БАЗА РЕАЛИЗАЦИИ КОНЦЕПЦИИ НУЛЕВОГО ДОВЕРИЯ

Аннотация. В статье представлена задача применения многоагентных систем при реализации концепции нулевого доверия. Обсуждаются возможные архитектуры многоагентных систем, используемых для решения задач сбора информации о состоянии системы, адаптации схем размещения точек применения политик безопасности. Рассматриваются особенности применения нейронной LSTM-сети в системе анализа сетевого трафика на уровне координации многоагентной системы.

Ключевые слова: концепция нулевого доверия, многоагентные системы, мониторинг состояния компьютерной сети, нейросетевые системы прогнозирования состояния характеристик системы.

S.S. Valeev, N.V. Kondratyeva, M.B. Guzairov, A.S. Ismagilova

MULTI-AGENT SYSTEMS AS A TECHNOLOGICAL BASIS FOR THE IMPLEMENTATION OF ZERO TRUST CONCEPT

Abstract. The paper considers the problem of applying multi-agent systems in the implementation of the concept of Zero Trust. Possible architectures of multi-agent systems used to solve the problems of collecting information about the state of the system, adapting the rules of the schemes for placing points of application of security policies are discussed. The features of the LSTM neural network application in the network traffic analysis system at the coordination level of a multi-agent system are considered.

Keywords: Zero Trust concept, multi-agent systems, computer network monitoring, neural network systems for predicting the state of system characteristics.

Введение

Как известно, ***мультиагентные системы*** (далее – МАС) представляют собой совокупность интеллектуальных программных агентов, которые кооперируются на основе протоколов обмена знаниями для достижения своих целей в рамках общей цели системы. Эти системы могут использоваться в различных областях, таких как робототехника, умный город, в том числе при решении задач кибербезопасности [1–3]. В контексте кибербезопасности МАС может использоваться для решения таких задач, как обнаружение вторжений, мониторинг сети и анализ системы на наличие вредоносных программ [4; 5].

Обнаружение вторжений является одной из актуальных задач в области кибербезопасности и включает в себя обнаружение необоснованной активности или несанкционированного доступа к компьютерной системе или сети [6–11]. Мультиагентная система решает эту задачу на основе кооперации нескольких агентов для одновременного мониторинга различных сегментов сети. Это позволяет ускорить обнаружение и реагирование на потенциальные угрозы за счет формирования обобщенного снимка состояния защищаемой системы [12].

Мониторинг текущего состояния сети является еще одним важным аспектом кибербезопасности. Это предполагает отслеживание всех действий, происходящих в сети, включая объем и структуру трафика, поведение пользователей и реализацию потенциальных угроз.

Валеев Сагит Сабитович
доктор технических наук, профессор, профессор кафедры управления информационной безопасностью, Уфимский университет науки и технологий, город Уфа. Сфера научных интересов: системы управления организационно-техническими объектами, информационные технологии, защита информации. Автор более 150 опубликованных научных работ. SPIN-код: 7137-0688, AuthorID: 111063.
Электронный адрес: vss2000@mail.ru

Кондратьева Наталья Владимировна
кандидат технических наук, доцент, доцент кафедры информатики, Уфимский университет науки и технологий, город Уфа. Сфера научных интересов: системы управления организационно-техническими объектами, информационные технологии. Автор более 80 опубликованных научных работ. SPIN-код: 7019-0617, AuthorID: 698412.
Электронный адрес: knv24@mail.ru

Гузаиров Мурат Бакеевич
доктор технических наук, профессор, профессор кафедры управления информационной безопасностью, Уфимский университет науки и технологий, город Уфа. Сфера научных интересов: информационные технологии, защита информации, анализ сложных систем. Автор более 400 опубликованных научных работ. SPIN-код: 3582-5594, AuthorID: 156078.
Электронный адрес: Mbguzairov@gmail.com

Исмагилова Альбина Сабирьяновна
доктор физико-математических наук, доцент, заведующий кафедрой управления информационной безопасностью, Уфимский университет науки и технологий, город Уфа. Сфера научных интересов: информационные технологии, математическое моделирование, защита информации. Автор более 150 опубликованных научных работ. SPIN-код: 8482-9719, AuthorID: 332892.
Электронный адрес: ismagilovaas@yandex.ru

МАС в данном контексте может быть полезной при кооперации нескольких агентов для одновременного (синхронизированного) анализа различных частей сети, выявления вредоносного программного обеспечения (далее – ПО). В ряде случаев это позволяет ускорить процесс анализа, что, в свою очередь, позволяет лучше понять возможности вредоносного ПО [13].

Многоагентные системы и концепция нулевого доверия

Концепция нулевого доверия (англ. Zero Trust) – это подход к безопасности, когда предполагается, что ни один пользователь, устройство или приложение не имеют доверия автоматически даже в демилитаризованной зоне, пока не будет доказана его легитимность при обращении к активам в сети [14; 15].

МАС и концепция нулевого доверия (далее – КНД) могут эффективно использоваться вместе для повышения уровня кибербезопасности.

В контексте МАС концепция Zero Trust может быть применена для решения следующих основных задач защиты информации.

Аутентификация и авторизация. Каждый агент в МАС должен быть аутентифицирован и авторизован перед доступом к ресурсам или выполнением задач. Это может включать проверку учетных данных, сертификатов или других механизмов аутентификации.

Контроль доступа. Доступ к ресурсам и данным должен быть ограничен и контролироваться. Агенты должны иметь только те права доступа, которые необходимы для выполнения их задач.

Мониторинг и аудит. Все действия агентов должны быть отслеживаемы и записаны в журнал аудита. Это позволяет быстро обнаруживать и реагировать на любые подозрительные активности.

Обнаружение угроз. В МАС могут использоваться различные методы обнаружения угроз, такие как сигнатурный анализ, поведенческий анализ и машинное обучение.

Защита коммуникаций. Коммуникации между агентами должны быть защищены с помощью шифрования и других методов защиты информации.

Автоматизация процессов. Некоторые аспекты безопасности, такие как мониторинг, обнаружение угроз и реагирование, могут быть автоматизированы с помощью агентов, что повышает эффективность и скорость реакции на угрозы.

Применение КНД в МАС помогает повысить уровень безопасности системы, уменьшить риски и обеспечить более надежную защиту от злоумышленников и различных кибератак на активы предприятия.

На Рисунке 1 представлена обобщенная архитектура МАС для решения задач в рамках КНД. Система является надстройкой над системным слоем, реализующим методы M_i $(i = 1{:}\ n)$ защиты функции.

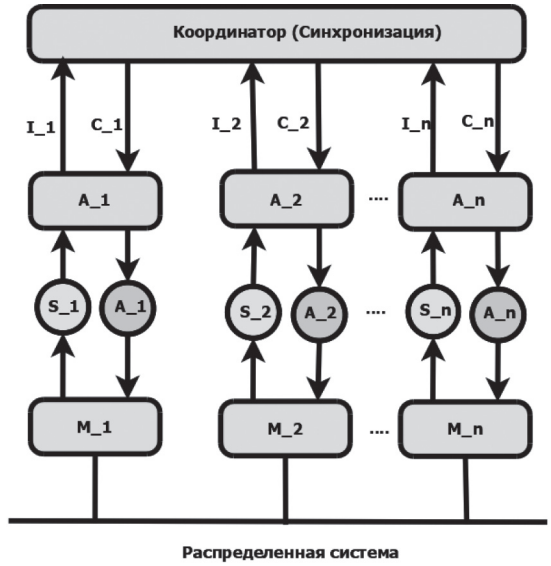

Рисунок 1. Многоагентная система для реализации концепции нулевого доверия
Источник: здесь и далее рисунки выполнены авторами.

Информация о состоянии системы собирается с помощью набора сенсоров S_i $(i = 1{:}\ n)$ и передается агенту A_i $(i = 1{:}\ n)$, связанному с уровнем координации. Поступающая информация на уровне координации обрабатывается агентом, который рекомендует агенту использование i-го метода защиты.

Основные задачи, решаемые МАС в контексте концепции нулевого доверия

Рассмотрим набор основных методов для адаптации точек применения политик безопасности:

• при обнаружении любых подозрительных действий или несанкционированного доступа к компьютерной системе или сети применяется многофакторная аутентификация;

• при мониторинге активности в сети отслеживаются все процессы, происходящие в сети, включая изменение трафика, поведение пользователей и потенциальные угрозы;

• анализ возможного использования вредоносного программного обеспечения включает оценку цели внедряемого программного обеспечения, его функциональных возможностей и потенциального воздействия на систему или сеть.

С учетом распределенного характера применения КНД использование МАС имеет неоспоримые преимущества:

• быстрое обнаружение и реагирование. Благодаря использованию нескольких агентов для мониторинга различных частей сети одновременно МАС позволяет быстрее обнаруживать и реагировать на угрозы;

• лучшее покрытие защищаемой сети. МАС обеспечивает лучшее покрытие всей сети, так как каждый агент может обеспечивать защиту на своей части сети;

• более полное наблюдение. МАС позволяет проводить более полное наблюдение за сетью, так как каждый агент может собирать данные о своей части сети;

• улучшенные возможности анализа. МАС позволяет проводить более глубокий анализ вредоносного ПО, так как каждый агент может анализировать свою часть анализируемого кода распределенной системы для *i*-го метода защиты.

Особенности реализации МАС в решении задачи защиты информации в рамках концепции нулевого доверия

Реализация МАС может быть выполнена различными способами в зависимости от требований и целей проекта. Рассмотрим основные этапы проектирования МАС.

Этап 1. Определение целей и задач системы. Необходимо четко определить, какие задачи должна решать система и какие функции она должна выполнять.

Этап 2. Разработка архитектуры системы. На данном этапе определяется структура системы, количество и типы агентов, их взаимодействие друг с другом и окружающей средой.

Этап 3. Разработка агентов. Каждый агент должен быть спроектирован таким образом, чтобы он мог выполнять свои задачи и взаимодействовать с другими агентами. Это включает разработку алгоритмов принятия решений, планирования действий и коммуникации.

Этап 4. Разработка среды взаимодействия. Необходимо создать среду, в которой будут работать агенты.

Этап 5. Тестирование и отладка. После разработки системы необходимо провести тестирование каждого агента и всей системы в целом. Это поможет выявить ошибки и улучшить работу системы.

Этап 6. Оптимизация и улучшение. После запуска системы необходимо продолжать ее оптимизацию и улучшение, основываясь на данных, полученных в процессе работы.

Этап 7. Поддержка и обновление. Система должна поддерживаться и обновляться в соответствии с новыми требованиями и изменениями в окружающей информационной среде.

Создание агента, например, на языке Python, может быть довольно сложным процессом, поскольку это требует использования множества различных библиотек и фреймворков, таких как Tensor Flow, Keras, Py Torch и др.

В качестве системы поддержки принятия решений предлагается использовать ***нейронную сеть LSTM*** (см. Рисунок 2). Данный тип сетей позволяет решать задачи прогнозирования поведения временных рядов с достаточно высокой точностью. Для реализации нейросетевой поддержки принятия решений МАС формирует тестовые наборы (datasets) за определенный период времени. Далее эти данные используются для обучения нейронной сети LSTM на уровне координации. Агентам нижнего уровня передается обученная сеть. В случае обнаружения аномалий трафика на верхний уровень от агентов передаются сигналы, которые анализируются координатором. На основе анализа результатов сигналов принимается решение об адаптации политики безопасности в точках их применения.

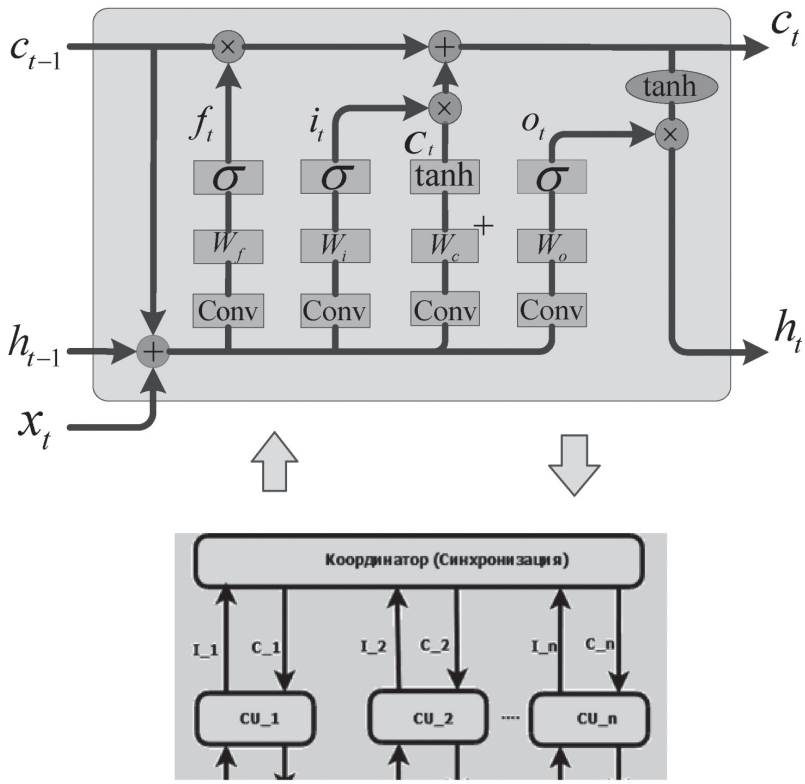

Рисунок 2. Нейронная LSTM-сеть, используемая в системе анализа сетевого трафика на уровне координации МАС

Следует отметить, что множество агентов, реализованных в системе, не должны в значительной мере влиять на эффективность защищаемой системы, что, к сожалению, не всегда возможно обеспечить, так как дополнительный слой анализа и принятия решений требует дополнительных ресурсов защищаемой вычислительной системы.

Заключение

Рассмотрены особенности многоагентных технологий применительно к решению задач защиты информации в рамках концепции нулевого доверия. Обсуждаются достоинства и недостатки применения многоагентных технологий для решения задач защиты информации предприятия при адаптации точек применения политик безопасности. Пред-

ложена обобщенная архитектура многоагентной системы защиты информации, включающая средства анализа состояния системы, набор агентов и правила их взаимодействия. В качестве системы поддержки принятия решений рекомендована к использованию нейронная сеть LSTM. В качестве ограничения применения многоагентных технологий отмечается необходимость привлечения дополнительных ресурсов защищаемой системы.

Литература

1. *Salamon T.* Design of Agent-Based Models: Developing Computer Simulations for a Better Understanding of Social Processes. Prague : Bruckner Publishing, 2011. 208 p. ISBN 978-80-904661-1-1.

2. *Russell S.J., Norvig P.* Artificial Intelligence: A Modern Approach. 2nd edition. Upper Saddle River, New Jersey : Prentice Hall, 2003. 1080 p. ISBN 0-13-790395-2.

3. *Fasli M.* Agent-technology for E-commerce. John Wiley & Sons, 2007. 480 p. ISBN 978-0-470-03030-1.

4. *Cao L., Gorodetsky V., Mitkas P. A.* Agent Mining: The Synergy of Agents and Data Mining // IEEE Intelligent Systems. 2009. Vol. 24. No. 3. Pp. 64–72. DOI: 10.1109/MIS.2009.45

5. *Поздняк И.С., Макаров И.С.* Модели обнаружения атак с использованием методов машинного обучения // Вестник Российского нового университета. Серия: Сложные системы: модели, анализ и управление. 2024. № 1. С. 99–109. EDN MNMSYZ. DOI: 10.18137/Rnu.v9187.24.01.p.99

6. *Rose S., Borchert O., Mitchell S., Connelly S.* Zero Trust Architecture. NIST Special Publication 800-207. Gaithersburg : National Institute of Standards and Technology, 2020. DOI: https://doi.org/10.6028/NIST.SP.800-207

7. *Singh R., Srivastav G., Kashyap R., Vats S.* Study on Zero-Trust Architecture, Application Areas & Challenges of 6G Technology in Future // Proceedings of 2023 International Conference on Disruptive Technologies (ICDT). Greater Noida, India, May 11–12, 2023. P. 375–380. DOI: 10.1109/ICDT57929.2023.10150745

8. *Mandal D, Singhal N., Tyagi M.* Cybersecurity in the Era of Emerging Technology // Emerging Technology and Management Trends. Delhi : Manglam Publications, 2023. P. 108–134.

9. *Гвоздев В.Е., Гузаиров М.Б., Бежаева О.Я., Курунова Р.Р., Насырова Р.А.* Информационная поддержка проактивного управления функциональной безопасностью компонентов киберфизических систем // Моделирование, оптимизация и информационные технологии. 2020. Т. 8. № 2 (29). EDN WZQQDR. DOI: 10.26102/2310-6018/2020.29.2.018

10. *Золотухина М.А., Зыков С.В.* Исследование и определение признаков скрытых атак на предприятии для алгоритмов машинного обучения // Вестник российского нового университета. Серия: Сложные системы: модели, анализ и управление. 2023. № 1. С. 20–28. EDN IMHLSV. DOI: 10.18137/RNU.V9187.23.01.P.20

11. *Глухих И.Н., Глухих Д.И., Карякин Ю.Е.* Представление и отбор ситуаций на сложном технологическом объекте в условиях неопределенности // Вестник российского нового университета. Серия: Сложные системы: модели, анализ и управление. 2021. № 2. С. 65–73. EDN LIPAMO. DOI: 10.25586/RNU.V9187.21.02.P.065

12. *Валеев С.С., Кондратьева Н.В.* Особенности проектирования систем безопасности на базе архитектуры нулевого доверия // Инженерный вестник Дона. 2023. № 8. С. 223–230. EDN TBWJXY. URL: https://ivdon.ru/ru/magazine/archive/n8y2023/8627 (дата обращения: 10.08.2024).

13. *Валеев С.С., Кондратьева Н.В.* Паттерны проектирования архитектуры нулевого доверия // Инженерный вестник Дона. 2023. № 9. С. 76–83. EDN FYJVBU. URL: https://ivdon.ru/ru/magazine/archive/n9y2023/8674 (дата обращения: 10.08.2024).

14. *Валеев С.С., Кондратьева Н.В., Гузаиров М.Б., Мельников А.В.* Этапы реинжиниринга информационной системы предприятия в рамках технологии нулевого доверия // Вестник российского нового университета. Серия: Сложные системы: модели, анализ и управление. 2023. № 3. С. 136–143. EDN PIDFBG. DOI: 10.18137/Rnu.v9187.23.03.p.136

15. *Валеев С.С., Кондратьева Н.В., Гузаиров М.Б., Исмагилова А.С.* Иерархическая динамическая система управления информационной безопасностью информационной системы предприятия // Инженерный вестник Дона. 2023. № 11. С. 154–164. EDN VBGGNG. URL: ivdon.ru/ru/magazine/archive/n11y2023/8802 (дата обращения: 10.08.2024).

References

1. Salamon T. (2011) *Design of Agent-Based Models: Developing Computer Simulations for a Better Understanding of Social Processes*. Bruckner Publishing. 208 p. ISBN 978-80-904661-1-1.

2. Russell S J., Norvig P. (2003) *Artificial Intelligence: A Modern Approach*. 2nd edition. Upper Saddle River, New Jersey : Prentice Hall. 1080 p. ISBN 0-13-790395-2.

3. Fasli M. (2007) *Agent-technology for E-commerce*. John Wiley & Sons. 480 p. ISBN 978-0-470-03030-1.

4. Cao L., Gorodetsky V., Mitkas P. A. (2009) Agent Mining: The Synergy of Agents and Data Mining. *IEEE Intelligent Systems*. Vol. 24. No. 3. Pp. 64–72.

5. Pozdnyak I.S., Makarov I.S. (2024) Attack detection models using machine learning methods. *Vestnik of the Russian New University. Series: Complex systems: Models, analysis and control*. No. 1. Pp. 99–110. DOI: 10.18137/Rnu.v9187.24.01.p.99. (In Russian).

6. Rose S., Borchert O., Mitchell S., Connelly S. (2020) *Zero Trust Architecture. NIST Special Publication 800-207*. Gaithersburg : National Institute of Standards and Technology. DOI: https://doi.org/10.6028/NIST.SP.800-207

7. Singh R., Srivastav G., Kashyap R., Vats S. (2023) Study on Zero-Trust Architecture, Application Areas & Challenges of 6G Technology in Future. In: *2023 International Conference on Disruptive Technologies (ICDT)*. Greater Noida, India, May 11–12, 2023. Pp. 375–380. DOI: 10.1109/ICDT57929.2023.10150745

8. Mandal D, Singhal N., Tyagi M. (2023) Cybersecurity in the Era of Emerging Technology. In: *Emerging Technology and Management Trends*. Delhi : Manglam Publications. Pp. 108–134.

9. Gvozdev V.E., Guzairov M.B., Bezhaeva O.Ya., Kurunova R.R., Nasyrova R.A. (2020) Information support for proactive management of functional safety of components of cyber-physical systems. *Modeling, Optimization, and Information Technology*. Vol. 8. No. 2 (29). DOI: 10.26102/2310-6018/2020.29.2.018 (In Russian).

10. Zolotukhina M.A., Zykov S.V. (2023) Investigation and identification of signs of hidden attacks in the enterprise for machine learning algorithms. *Vestnik of the Russian New University. Series: Complex systems: Models, analysis and control*. No. 1. Pp. 20–28. DOI: 10.18137/RNU.V9187.23.01.P.20 (In Russian).

11. Glukhikh I.N., Glukhikh D.I., Karyakin Yu.E. (2021) Representation and retrieve of the situation on a complex technological object in the uncertainty conditions. *Vestnik of the Russian New University. Series: Complex systems: Models, analysis and control*. No. 2. Pp. 65–73. DOI: 10.25586/RNU.V9187.21.02.P.065 (In Russian).

12. Valeev S.S., Kondratieva N.V. (2023) Features of designing security systems based on zero-trust architecture. *Engineering Journal of Don*. No. 8. Pp. 223–230. URL: https://ivdon.ru/ru/magazine/archive/n8y2023/8627 (accessed 10.08.2024). (In Russian).

13. Valeev S.S., Kondratieva N.V. (2023) Zero Trust Architecture Design Patterns. *Engineering Journal of Don*. No. 9. Pp. 76–83. URL: https://ivdon.ru/ru/magazine/archive/n9y2023/8674 (accessed 10.08.2024). (In Russian).

14. Valeev S.S., Kondratieva N.V., Guzairov M.B., Melnikov A.V. (2023) Stages of reengineering the information system of the enterprise within the framework of Zero Trust technology. *Vestnik of the Russian New University. Series: Complex systems: Models, analysis and control*. No. 3. Pp. 136–143. DOI: 10.18137/Rnu.v9187.23.03.p.136 (In Russian).

15. Valeev S.S., Kondratieva N.V., Guzairov M.B., Ismagilova A.S. (2023) Hierarchical dynamic information security management system of the enterprise information system. *Engineering Journal of Don*. No. 11. Pp. 154–164. URL: ivdon.ru/ru/magazine/archive/n11y2023/8802 (accessed 10.08.2024). (In Russian).