УДК 004.056

А. М. Малькута[1]*

Исследование алгоритмов реагирования на события в информационной системе, построенных по образу спинальных рефлексов

[1] Национальный исследовательский ядерный университет «МИФИ», г. Москва, Российская Федерация
* e-mail: AMMalkuta@mephi.ru

Аннотация. Данное исследование направлено на анализ и сравнение существующих алгоритмов реагирования на события в информационной системе, которые основаны на принципах спинальных рефлексов. Спинальные рефлексы представляют собой автоматические движения, которые вызываются определенными стимулами без участия коры головного мозга. Перенос данных принципов на информационные системы позволяет создать более эффективные и быстрые алгоритмы управления сетями, обработки событий и выявления проблем. В данной работе будет произведен обзор различных подходов к моделированию спинальных рефлексов и их применение в информационных системах. Будут рассмотрены методы их интеграции в алгоритмы управления и мониторинга сетей. Результаты исследования позволят определить перспективные направления для развития алгоритмов реагирования на события в информационных системах по образу спинальных рефлексов, а также выявить преимущества и недостатки различных подходов.

Ключевые слова: DevOps, конфигурирование, автоматизация, информационная безопасность, интеллектуально-адаптивное управление, Ansible

A. M. Malkuta[1]*

Research of Algorithms of Response to events in the Information System Built on the Image of Spinal Reflexes

[1] National Research Nuclear University MEPhI (Moscow Engineering Physics Institute), Moscow, Russian Federation
* e-mail: AMMalkuta@mephi.ru

Abstract. This research aims to analyze and compare existing algorithms for responding to events in an information system, which are based on the principles of spinal reflexes. Spinal reflexes are automatic movements that are triggered by certain stimuli without the involvement of the cerebral cortex. Transferring these principles to information systems allows for more efficient and faster algorithms for network management, event processing and problem detection. This paper will review various approaches to modelling spinal reflexes and their application in information systems. Methods of their integration into network control and monitoring algorithms will be discussed, as well as their effectiveness and applicability to specific tasks. The results of the study will help to identify promising directions for the development of algorithms for responding to events in information systems in the image of spinal reflexes, as well as to identify the advantages and disadvantages of different approaches.

Keywords: DevOps, configuration, automation, information security, intelligent adaptive management, Ansible

Введение

В современном мире информационная безопасность играет центральную роль в обеспечении устойчивости и безопасности организаций, государств и отдельных граждан. Комплексные меры по защите информации от киберугроз, утечек данных и хакерских атак становятся все более необходимыми в условиях быстрого развития технологий и интернета.

Уровень информационной безопасности определяет степень конфиденциальности, целостности и доступности данных, что важно как для защиты частной жизни граждан, так и для обеспечения бесперебойной работы организаций и государственных структур. Нарушение информационной безопасности может привести к нежелательным последствиям для компании или государственной структуры, включая финансовые и репетиционные потери, утечку конфиденциальных данных и появление угроз самому существованию предприятия. Поэтому развитие комплексных систем информационной безопасности, включающих в себя технические, организационные и правовые меры, становится одним из приоритетов для обеспечения стабильности и безопасности в современном мире [1].

Частью комплекса информационной безопасности являются алгоритмы реагирования на события в системе. Это специальные процедуры, которые определяют, как система должна реагировать на определенные события [2]. Подобные алгоритмы обычно включают в себя определение условий события, его обработку и выполнение определенных действий в ответ на это событие. Например, алгоритмы могут включать в себя процедуры обработки ошибок, уведомления пользователей, выполнение автоматических действий и другие действия, которые помогают системе функционировать более эффективно и безопасно. Важно чтобы алгоритмы реагирования на события были оптимизированы и эффективны, и система могла быстро отслеживать и обрабатывать различные события [3].

Таким образом можно провести аналогию со спинальными рефлексами. Это автоматические движения, которые возникают в ответ на воздействие раздражителя на соответствующие рецепторы в коже, сухожилиях или мышцах. Они происходят без участия головного мозга и контролируются спинным мозгом. Спинальные рефлексы необходимы для поддержания равновесия и защиты организма от внешних воздействий [4]. Примером безусловного рефлекса является рефлекс коленного сухожилия. Он происходит при ударе по колену и вызывает сокращение четырехглавой мышцы бедра и растяжение тендона (рис. 1). Условные же рефлексы требуют участие головного мозга, тем самым растягивая процесс, что в некоторых случая необходимо и обосновано. Выделение слюны при виде и запахе пищи является примером подобного биологического процесса (рис. 2). Так, спинальные процессы отличаются автоматизмом и скоростью, что крайне важно в рамках системы информационной безопасности предприятия.

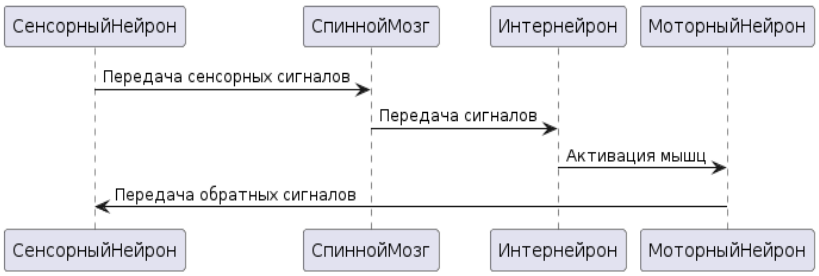

Рис. 1. Пример диаграммы спинального рефлекса

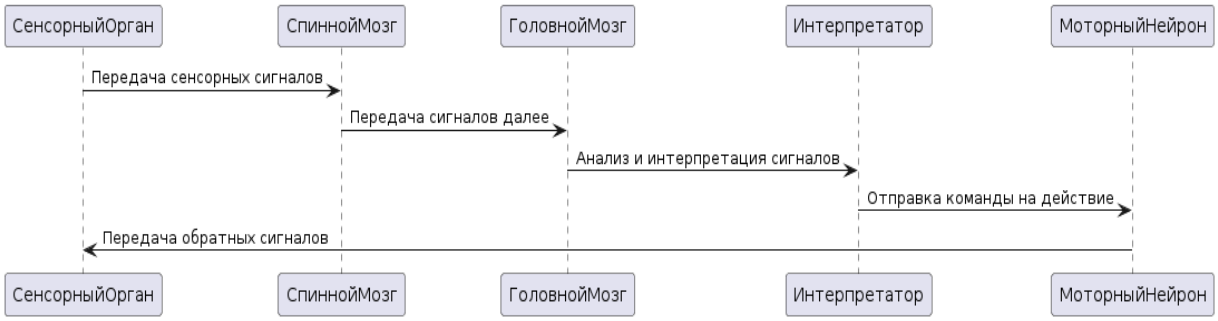

Рис. 2. Пример диаграммы условного рефлекса

Исследование

Реагирование на события является ключевым аспектом работы информационных систем, поскольку позволяет им быть более гибкими, адаптивными и эффективными. Для более глубокого понимания важности этого аспекта следует привести несколько примеров, демонстрирующих важность реагирования на события в информационной системе.

Информационная система должна быть способна мгновенно реагировать на подозрительную активность или атаки, чтобы обеспечить безопасность данных и инфраструктуры [5]. Так, система мониторинга безопасности может автоматически блокировать доступ пользователя при обнаружении необычной активности или попыток взлома.

В электронной коммерции важно быстро реагировать на события, такие как увеличение спроса на определенный товар или изменение цен у конкурентов. Система автоматизированного управления ценами может немедленно пересчитать цены на товары в реальном времени с учетом изменений на рынке.

В интернете вещей события могут происходить очень быстро и в большом количестве, что требует оперативной реакции [6]. Например, смарт-дом может мгновенно реагировать на определенные события, такие как срабатывание датчика движения или изменение погоды, выполняя заданные действия, например, включение света или регулировка температуры.

В целом, реагирование на события в информационных системах не только улучшает их производительность, но и позволяет им адаптироваться к изменениям внешней среды и предоставлять более качественный сервис пользователям.

Это особенно актуально в условиях постоянно растущих киберугроз для предприятий.

В 2023 году Центр информационной безопасности компании «Инфосистемы Джет» сообщил о росте числа кибератак на 11% по сравнению с предыдущим годом [7].

Основные выводы отчета:

– наиболее распространенными типами кибератак были заражение вредоносным ПО через посещение опасных сайтов и фишинговые атаки;

– у 72 % компаний были обнаружены критические уязвимости во внешней инфраструктуре, что может быть использовано злоумышленниками для проникновения в системы компании;

– более 90 % компаний столкнулись с утечками учетных данных сотрудников. В большинстве случаев утечки включали логины и пароли или хэши паролей, что позволяет злоумышленникам взламывать учетные записи;

– 93 % компаний, которые использовали услугу мониторинга внешних угроз от «Инфосистемы Джет», упоминались на форумах и каналах хакеров в даркнете, что указывает на интерес злоумышленников к этим компаниям.

Рассмотрим подробнее реагирование на инциденты информационной системы в рамках комплекса безопасности предприятия. Оно является критической частью комплексной стратегии информационной безопасности для защиты систем и данных от всего спектра существующих угроз [8].

Процесс реагирования на события обычно включает следующие этапы:

– обнаружение и идентификация потенциальной киберугрозы или инцидента [9];

– оценка серьезности и масштабов угрозы или инцидента для определения соответствующих действий;

– принятие мер для предотвращения дальнейшего распространения или ущерба от угрозы или инцидента;

– удаление или исправление угрозы или инцидента для восстановления нормальной работы системы;

– восстановление систем и данных до их первоначального состояния или до приемлемого уровня функционирования;

– запись подробностей инцидента и предпринятых действий для справки и анализа.

В рамках проведения всех этих этапов система может требовать участия оператора или работать самостоятельно согласно прописанным алгоритмам и инструкциям. Подобная интерпретация позволяет провести аналогию со спинальным рефлексом, в рамках работы которого не требуется вмешательство головного мозга для реагирования на раздражитель, а в случае комплекса информационной безопасности может не требоваться согласование с оператором (головным мозгом). Наличие человека в системе также ведет к появлению новых угроз и дает новые возможности для нанесения вреда предприятию [10]. В связи с этим возникает потребность в выявлении «спинного мозга» комплекса ИБ

предприятия. Подобным автоматическим обработчиком может послужить доверенный искусственный интеллект, обученный работе с угрозами информационной безопасности в различных плоскостях [11]. Дабы разгрузить этот механизм безопасности, имеет смысл проводить разработку отдельных ИИ для каждого поля задач, от сетевой инфраструктуры предприятия до целостности системы безопасности отдельной части системы [12, 13, 14].

Спинальные рефлексы в связке с ИИ можно интегрировать в комплекс информационной безопасности предприятия двумя основными способами (на примере сетевых алгоритмов):

– прямая интеграция, которая подразумевает, что безусловные рефлексы встраиваются непосредственно в алгоритмы управления сетью. Система может использовать рефлекс (автоматику) для немедленного переключения на резервный маршрут, если основной маршрут выходит из строя;

– интеграция на примере моделирования. Происходит построение спинальных рефлексов с помощью математических моделей, которые затем включаются в сетевые алгоритмы. Это позволяет настраивать ИИ для конкретных сетевых условий и подстраивать их под действующие на данный момент угрозы, что дает системе возможность проводить своего рода самоорганизацию [15].

Более конкретным может послужить пример автоматизации конфигурирования сети предприятия с учетом возникших угроз. ИИ обрабатывает полученную информацию, которая может поступить в ходе атаки на часть системы или рассылаться оператором самостоятельно, и производит переконфигурирование других участков сети предприятия с помощью системы управления Ansible, генерируя нужные сценарии [16].

Заключение

Таким образом, в данной работе была разобрана работа алгоритмов интеллектуального реагирования на инциденты информационной системы предприятия, а также сформулирована гипотеза о возможности работы подобных алгоритмов согласно принципам спинальных рефлексов в человеческом организме. Интеграция безусловных рефлексов в алгоритмы работы комплекса информационной безопасности имеет ряд преимуществ, среди которых быстрое реагирование, увеличенная стойкость системы, уменьшенная задержка реакции и упрощенное управление комплексом в целом.

Важно отметить, что исследование данной тематики необходимо углублять в связи с недостаточной проработанностью темы доверенного искусственного интеллекта, который смог бы заменить «спинной мозг» в системе, при этом не нанося ей вреда.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Ищенко, А. Н. Новая доктрина информационной безопасности Российской Федерации как основа противодействия угрозам безопасности России в информационной сфере / А. Н. Ищенко, А. Н. Прокопенко, А. А. Страхов // Проблемы правоохранительной деятельности. – 2017. – № 2. – С. 55-62.

2. Олейникова, А. А. Концепция управления информационной безопасностью на основе цикла непрерывного детектирования и реагирования на инциденты безопасности информации / А. А. Олейникова, В. В. Золотарев // Известия ЮФУ. Технические науки. – 2023. – № 5(235). – С. 66-81. – DOI 10.18522/2311-3103-2023-5-66-81.

3. Басыня, Е. А. Метод формирования децентрализованного реестра событий информационной инфраструктуры предприятия / Е. А. Басыня, А. В. Сафронов // Вестник Евразийского национального университета имени Л. Н. Гумилева. Серия: Технические науки и технологии. – 2022. – № 2(139). – С. 40-50.

4. Фонсова, Н. А. Анатомия центральной нервной системы : Учебник / Н. А. Фонсова, В. А. Дубынин, И. Ю. Сергеев. – 1-е изд.. – Москва : Издательство Юрайт, 2017. – 338 с. – (Профессиональное образование). – ISBN 978-5-534-00669-8.

5. Фирюлин, М. Е. система мониторинга и управления событиями информационной безопасности как часть комплексной системы защиты информации / М. Е. Фирюлин, Е. А. Родионов // Охрана, безопасность, связь. – 2019. – № 4-1. – С. 206-212.

6. Плынский, И. И. Система мониторинга климатических данных с использованием технологии интернета вещей / И. И. Плынский, В. И. Монахов // Молодые ученые - развитию Национальной технологической инициативы (ПОИСК). – 2020. – № 1. – С. 542-545.

7. Аналитический отчет о киберугрозах: итоги 2023 года // Jet CSIRT URL: https://jetcsirt.su/upload/godovoy_otchet__jet_2023.pdf (дата обращения: 16.04.2024).

8. Исследование IRP-систем на основе анализа механизмов реагирования на инциденты информационной безопасности / А. Р. Очередько, Д. А. Бачманов, М. М. Путято, А. С. Макарян // Прикаспийский журнал: управление и высокие технологии. – 2021. – № 1(53). – С. 74-82. – DOI 10.21672/2074-1707.2021.53.1.074-082.

9. Логинова, А. О. Классификация существующих методов выявления инцидентов информационной безопасности / А. О. Логинова // Информационные технологии в науке, бизнесе и образовании : Сборник трудов IX Международной научно-практической конференции студентов, аспирантов и молодых ученых, Москва, 01 декабря 2017 года. – Москва: Московский государственный лингвистический университет, 2017. – С. 40-44.

10. Малькута, А. М. Социальная инженерия - уязвимость современных систем / А. М. Малькута, В. Ю. Радыгин, Т. А. Манаенкова // Финансовая безопасность. Современное состояние и перспективы развития : Материалы VIII Международной научно-практической конференции Международного сетевого института в сфере ПОД/ФТ, Москва, 14–15 декабря 2022 года. Том 2. – Москва: Национальный исследовательский ядерный университет «МИФИ», 2022. – С. 305-310.

11. Никольская, К. Ю. Разработка методов доверенного искусственного интеллекта в сфере кибербезопасности / К. Ю. Никольская // Наука ЮУрГУ. Секции технических наук : материалы 74-й научной конференции, Челябинск, 19 апреля 2022 года – 21 2021 года / Министерство науки и высшего образования Российской Федерации Южно-Уральский государственный университет. – Челябинск: Издательский центр ЮУрГУ, 2022. – С. 291-297.

12. Гладунов, Д. С. Создание алгоритма реагирования на сетевые инциденты ИБ с использованием технологий машинного обучения / Д. С. Гладунов // Современные проблемы радиоэлектроники и телекоммуникаций. – 2023. – № 6. – С. 213.

13. Борисов, Н. С. Использование нейронных сетей в сфере информационной безопасности / Н. С. Борисов, С. А. Королев, А. И. Ядигаров // Инициативы молодых - науке и производству : Сборник статей VI Всероссийской научно-практической конференции молодых ученых и студентов, Пенза, 29–30 ноября 2023 года. – Пенза: Пензенский государственный аграрный университет, 2023. – С. 146-149.

14. Басыня, Е. А. Система интеллектуально-адаптивного управления информационной инфраструктурой предприятия / Е. А. Басыня // Информационные технологии. – 2020. – Т. 26, № 5. – С. 283-289. – DOI 10.17587/it.26.283-289.

15. Басыня, Е. А. Самоорганизующаяся система управления трафиком вычислительной сети / Е. А. Басыня, Г. А. Французова, А. В. Гунько // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2014. – № 1(31). – С. 179-184.

16. Unleashing Full Potential of Ansible Framework: University Labs Administration / P. Masek, M. Stusek, Ja. Krejci [et al.] // Conference of Open Innovations Association, FRUCT. – 2018. – No. 22. – P. 144-150.