N.A. Soloviov, N.A. Tishina, E.N. Chernoprudova

Multi-Agent Immune Anomaly Detection System for Cloud Environments

Keywords: Cloud, detection of anomalies, multi-agent immune systems.
In the article the architecture of the artificial immune system anomaly detection based on multi-agent with adjustable threshold of activation of reactive agents that will implement their adaptation to the conditions of cloud, ignore the random signals and detect the sequence of events is offered.

Н.А. Соловьев, Н.А. Тишина, Е.Н. Чернопрудова

МУЛЬТИАГЕНТНАЯ ИММУННАЯ СИСТЕМА ОБНАРУЖЕНИЯ АНОМАЛИЙ ОБЛАЧНОЙ СРЕДЫ

Введение

В настоящее время облачные технологии (Cloud Computing) переходят из сферы научных исследований в реальные бизнес-приложения, например, веб-сайты, облачные сервисы (малый бизнес, бухгалтерия) [1, 2]. Построение подобных распределенных приложений связывается с необходимостью обеспечения безопасности облачных серверов от различного рода аномалий. Под аномалией понимается любое отклонение от модели (профиля) нормального состояния информационных процессов облачных севисов. Отклонения вызываются сетевыми вторжениями: отказ обслуживания (DDoS), интернет-черви, сканирование, несанкционированный доступ (спам), а также сбоями (отказами) аппаратного обеспечения сети, некорректными действиями легитимных пользователей.

В настоящее время сложилась система методов, моделей и средств выявления аномалий информационных процессов телекоммуникационных сетей, разработаны общеметодологические принципы их использования, позволяющие решать широкий спектр задач информационной безопасности (ИБ). Сетевые системы обнаружения аномалий (ANIDS – Anomaly based network intrusion detection systems) способны обнаруживать как известные, так и новые, ранее неизвестные аномалии, в отличие от систем обнаружения вторжений (NIDS – network intrusion detection systems), основанных на сигнатурных методах (SPADE, PHAD, ALAD, LERAD) [2–5].

Учитывая особенности облачной среды (распределенные сервера, находящиеся в разных сегментах сети, включая пространственное распределение, динамическое изменение количества виртуальных серверов и потребляемых вычислительных ресурсов), изменяются базовые требования к ANIDS, которыми становятся: автоматическая адаптация ANIDS под размеры облачной среды и наличие гибкой системы коммуникации между серверами, распределенная база сигнатур известных аномалий, автономность сервера при отсутствии связи с другими серверами, обнаружение новых видов аномалий (угроз) и своевременное распространение информации о них, минимальное потребление ресурсов на систему защиты.

В связи с постоянным ростом числа известных фактов нарушения целостности и доступности информации в облачной среде, возникает необходимость разработки принципиально иных подходов к обеспечению ИБ, позволяющих обнаруживать аномалии неизвестных ранее типов в условиях ограничения на потребляемые ресурсы. Это определяет *актуальность* проведения исследований в области теоретико-эксперимен-

тального обоснования системы автоматической идентификации аномалий облачной среды.

Одним из наиболее перспективных направлений развития систем обнаружения аномалий в условиях новых требований считается использование искусственных иммунных систем (artificial immune system – AIS), основанных на принципах иммунной системы человека [3–5]. Использование AIS обеспечивает свойства, характерные иммунной системе человека, которыми должна обладать ANIDS облачной среды: распределенность, самоорганизуемость и ресурсосбережение.

Современное антивирусное программное обеспечение уже использует некоторые принципы AIS для обнаружения вирусных сигнатур по шаблонам [5], но большинство коммерческих продуктов не имеют функционала адаптивной иммунной системы для обнаружения неизвестных аномалий облачной среды.

Программная реализация мультиагентной иммунной системы защиты облачной среды

Развитие искусственных иммунных систем для обнаружения аномалий облачной среды предлагается реализовать на основе идей мультиагентности [2]. Построение мультиагентной искусственной иммунной системы обнаружения аномалий облачной среды на базе распределенных интеллектуальных агентов (Мультиагентные искусственные иммунные системы, англ. Multi-agent artificial immune system – MAAIS), позволит реализовать распределенность, интеллектуальность, адаптацию к изменяющейся среде и коммуникативные способности компонентов иммунной системы.

На рис. 1 представлена архитектура программного проекта MAAIS в виде диаграммы компонентов, показывающей зависимости между различными типами компонент системы.

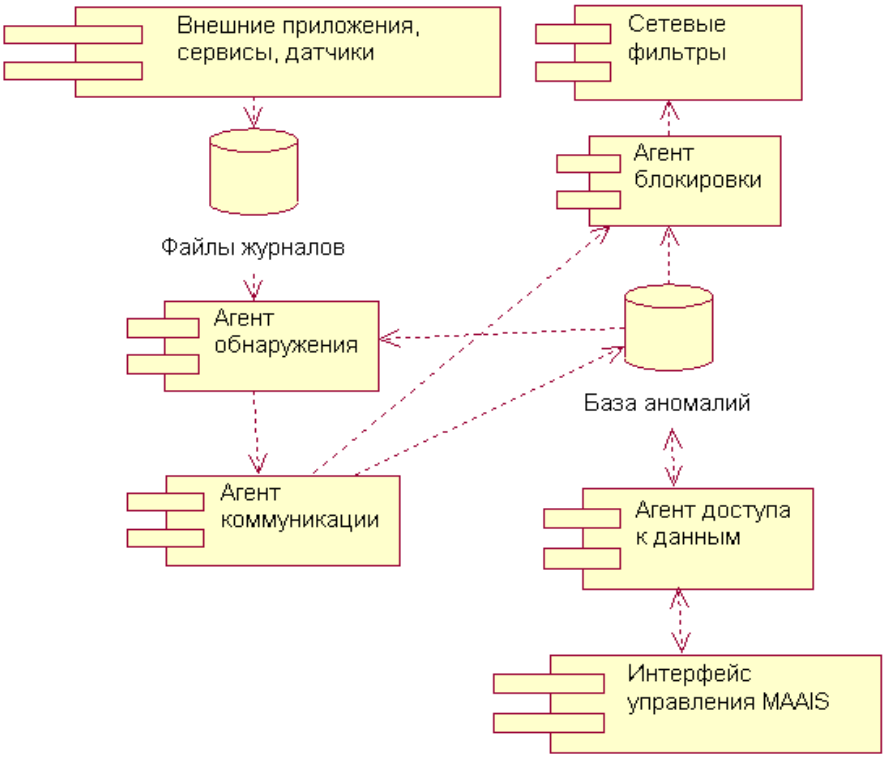

Рис. 1. Диаграмма компонентов MAAIS

Основными компонентами MAAIS являются интеллектуальные агенты обнаружения, агенты иммунного ответа (блокировки) и агенты коммуникации, предложенные в [2].

Для корректной работы распределенной системы MAAIS данные о текущих аномалиях и существующих сигнатурах должны храниться на каждом узле мультиагентной сети. Данные представляют структуру таблиц, не связанных друг с другом, но для высоконагруженной системы (облака) количество данных достигает больших объемов, что может приводить к замедлению их выборки и анализа. Поэтому применение традиционных реляционных СУБД нецелесообразно, так как потребует дополнительных ресурсов для работы MAAIS.

Из-за фиксированных таблиц ключ-значение и ограниченных функций MAAIS в качестве хранилища данных выбрана документо ориентированная СУБД MongoDB, состоящая из следующих таблиц: маска событий (код, первичная маска, дополнительные условия, тип аномалии, аномалия, уровень сигнала опасности); сигнатура трафика (код, первичная сигнатура, дополнительные условия, тип аномалии, аномалия, уровень сигнала опасности); сигнатура аномалии (IP-адрес, уровень опасности, текущий статус, обнаруженные маски, обнаруженные сигнатуры).

Для интерфейса управления MAAIS дополнительно предусмотрена вспомогательная реляционная база данных (БД), предназначенная для сбора статистики работы MAAIS, отображения событий, построения отчетов и хранения таблицы прав доступа. Для взаимодействия MAAIS и интерфейса управления предусмотрен дополнительный служебный **агент доступа к данным.** Агент функционирует аналогично агенту коммуникации, но без алгоритмов расчета уровня опасности. Основные задачи агента доступа к данным: оповещение агентов коммуникации об изменениях списков доступа; прием сигналов об обнаруженных аномалиях и событиях блокировки источника угроз, обеспечивающих запись событий в базу данных для дальнейшего анализа; рассылка событий наблюдающим администраторам.

Модель агента обнаружения. Агенты обнаружения собирают сигналы, агрегируют их и передают агентам коммуникации для дальнейшего анализа и принятия решения о блокировке. В процессе обнаружения не требуется сохранение состояния, поэтому агент реализован реактивным, диаграмма классов которого представлена на рис. 2.

Модель агента коммуникации. Агенты коммуникации, на основании собранной информации от агентов обнаружения и других агентов коммуникации, производят вычисление уровня опасности по каждому IP-адресу и принимают решение о блокировке, соответствующий сигнал передается агентам блокировки, которые в свою очередь управляют сетевыми фильтрами и (или) карантинными зонами. Принятие решения о блокировке источника аномалий происходит на основе модели настраиваемого порога активации, методика формирования которого изложено в [2, 7]. Агент коммуникации, отвечающий за вычисление уровня опасности, накапливает информацию по каждому адресу клиента и сообщает другим агентам об обнаруженных аномалиях. В терминологии MAAIS агент коммуникации представлен BDI-архитектурой и имеет убеждения, желания и намерения. Диаграмма классов BDI-агента коммуникации представлена на рис. 3.

Модель агента блокировки. Агенты блокировки (иммунного ответа) – реализуют механизмы блокировки клиентов на основе сигнатур, полученных от агентов коммуникации (из базы сигнатур), управляя сетевыми фильтрами. Аналогично агенту обнаружения реализован как реактивный агент, не обладающий внутренним преставлением внешней среды.

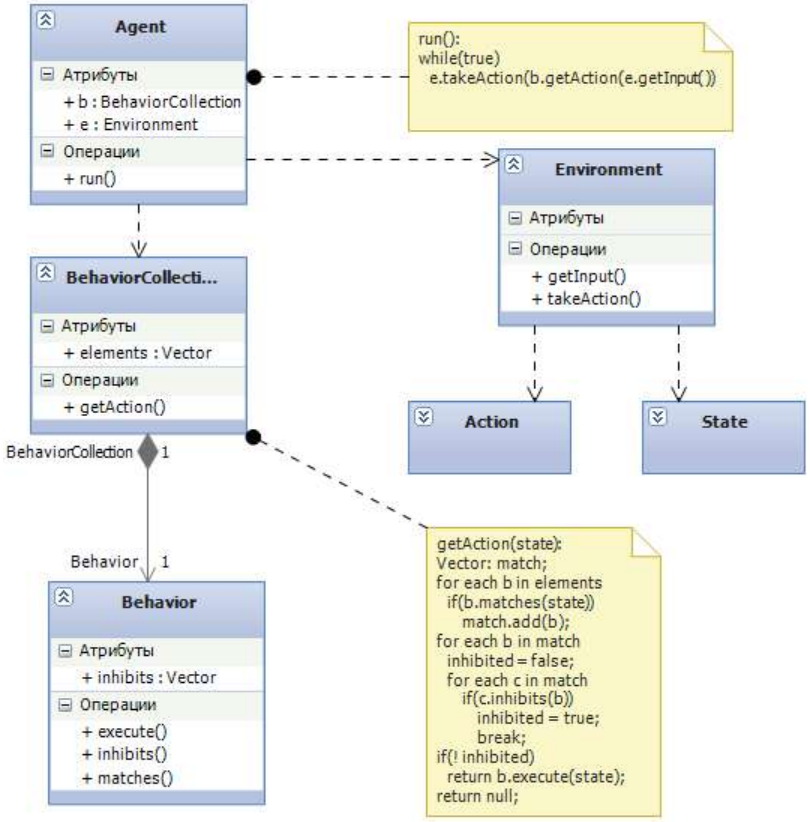

Рис. 2. Диаграмма классов реактивного агента обнаружения

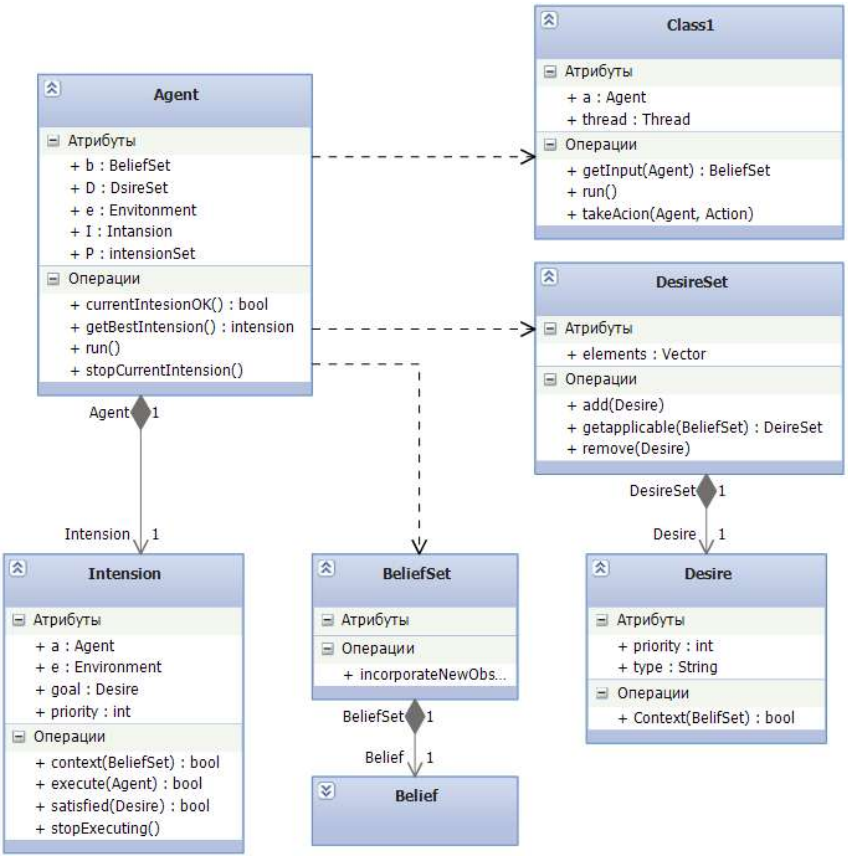

Рис. 3. Диаграмма классов BDI-агента коммуникации

На основе представленных диаграмм разработан прототип системы ANIDS – MAAIS для обеспечения безопасности облачной среды, позволяющей обнаруживать следующие виды аномалий: отказ в обслуживании; обход системы авторизации; повышение привилегий; поиск уязвимостей программного обеспечения.

Экспериментальная оценка предложенной MAAIS

В настоящее время в мировой практике накоплен опыт эксплуатации ANIDS, на основании которого сформировался комплекс критериев и оценок работы подобных систем [2, 4]. В то же время основная масса методов нацелена на изучение поведения сосредоточенной телекоммуникационной сети, а для облачной среды возникают дополнительные частные показатели оценки системы обнаружения аномалий: вероятность пропуска аномалий; вероятность ложных срабатываний; успешность аномалий; пропускная способность сети (устойчивость к высокоинтенсивному трафику); устойчивость к обходу системы защиты; способность к обнаружению новых аномалий; коррелируемость аномалий; возможность коммуникации между агентами. На этапе эксперимента вероятности пропуска аномалий и ложного срабатывания становятся наиболее важными частными показателями MAAIS.

Экспериментальная оценка внедрения системы MAAIS использует известный способ тестирования систем обнаружения аномалий: воспроизведение реального трафика (1999 DARPA) и имитация программными средствами различных видов атак, знания о которых не заложены в базу MAAIS, что предполагает дальнейшую возможность обнаружения неизвестных угроз разработанной системой. Эксперимент (после верификации при помощи Valgrind в течение одного месяца) проводился с использованием инструментария имитации атак pytbull (300 тестов, сгруппированных в 11 модулей). В качестве дампов реального трафика использовались 1999 DARPA. В табл. 1 представлены результаты эксперимента по различным типам атак для сравнения основных характеристик разработанной MAAIS и системы ANIDS Snort.

Таблица 1. Сравнение характеристик разработанной системы MAAIS и Snort

Класс атак	Обнаружение аномалий, %		Ложные срабатывания, %	
	MAAIS	Snort	MAAIS	Snort
Отказ в обслуживании	98,1	97,2	2,9	2,8
Обход системы авторизации	93,7	94,5	2,3	4,6
Повышение привилегий	95,4	95,2	0,8	1,3
Поиск уязвимостей	97,6	96,2	1,7	3,5

Таким образом, разработанный прототип MAAIS не уступает по характеристикам распространенной системе предотвращения вторжений Snort, при этом работает в условиях экспериментальной облачной среды.

Заключение

Предложенный прототип MAAIS обеспечивает свойства, характерные иммунной системе человека, которыми должна обладать система обнаружения аномалий облачной среды: распределенность, самоорганизуемость и ресурсосбережение. Решение основано на принципах построения распределенной ANIDS путем интеграции искусственной иммунной системы с мультиагентным подходом. Прототип MAAIS адаптируется под меняющиеся параметры облачной среды и позволяет обнаруживать неизвестные ранее аномалии. Экспериментальная оценка внедрения предложенного прототипа

показала средний процент обнаружения 92% при вероятности ложной тревоги не более 0,05.

СПИСОК ЛИТЕРАТУРЫ:

1. Зегжда П.Д. Основные направления развития технологий обеспечения безопасности в эпоху информационного противоборства // Проблемы информационной безопасности компьютерных систем. 2007. № 1. С. 60 – 73.
2. Соловьев Н.А. Мультиагентная искусственная иммунная система блокировки источника угроз в облачной среде / Н.А. Соловьев, А.А. Щуров // Современные информационные технологии в науке, образовании и практике: материалы VIII всероссийской научно-практической конференции. Оренбург: ООО ИПК «Университет», 2012. С. 135–139.
3. Liu, S., Li, T., Wang, D., Zhao, K., Gong, X., Hu, X., Xu, C., Liang, G.: Immune Multiagent Active Defense Model for Network Intrusion. In: Wang, T.-D., Li, X.-D., Chen, S.- H., Wang, X., Abbass, H.A., Iba, H., Chen, G.-L., Yao, X. (eds.) SEAL 2006. LNCS, vol. 4247, pp. 101–111. Springer, Heidelberg (2006)
4. Fu, H., Yuan, X., Wang, N.: Multi-agents Artificial Immune System (MAAIS) Inspired by Danger Theory for Anomaly Detection. In: 2007 International Conference on Computational Intelligence and Security Workshops, pp. 570-573
5. Andrews P., Timmis J. Tunable Detectors for Articial Immune Systems: From Model to Algorithm // Bioinformatics for Immunomics (Ed. Springer). – 2010. – Vol. 3. – P. 103-127.
6. Искусственные иммунные системы и их применение. Artificial Immune Systems and Their Applications / Под ред. Д. Дасгупты; пер. с англ. А. А. Романюхи. М.: Физматлит, 2006.
7. Соловьев Н.А. Методика обнаружения аномалий облачной сре ды на основе модели настраиваемого порога активации / Н.А. Соловьев, Н.А. Тишина, Е.Н. Чернопрудова // Наука и образование: фундаментальные основы, технологии, инновации: материалы Международной научной конференции, посвященной 60-летию Оренбургского государственного университета. Оренбург: ООО ИПК «Университет», 2015. С. 248–253.

REFERENCES:

1. Zegzhda P.D. The Main directions of development of safety technologies in the era of information warfare // problems of information security of computer systems.2007. № 1. P. 60 – 73.
2. Soloviov N.A. Multi-agent artificial immune system block threats in the cloud environment / N.A. Soloviov, A.A. Shchurov // Modern information technologies in science, education and practice: materials of VIII all-Russian scientific-practical conference. Orenburg, «University», 2012. P. 135–139.
3. Artificial Immune Systems and Their Applications / edited D. Dasgupta; translation from English A. A. Romanucci. M.: Physmatlit, 2006. 344 p.
4. Liu, S., Li, T., Wang, D., Zhao, K., Gong, X., Hu, X., Xu, C., Liang, G.: Immune Multiagent Active Defense Model for Network Intrusion. In: Wang, T.-D., Li, X.-D., Chen, S.- H., Wang, X., Abbass, H.A., Iba, H., Chen, G.-L., Yao, X. (eds.) SEAL 2006. LNCS, vol. 4247, pp. 101–111. Springer, Heidelberg (2006).
5. Fu, H., Yuan, X., Wang, N.: Multi-agents Artificial Immune System (MAAIS) Inspired by Danger Theory for Anomaly Detection. In: 2007 International Conference on Computational Intelligence and Security Workshops, pp. 570-573.
6. Andrews P., Timmis J. Tunable Detectors for Articial Immune Systems: From Model to Algorithm // Bioinformatics for Immunomics (Ed. Springer). 2010. Vol. 3. Pp. 103-127.
7. Soloviev, N.A The method for detecting anomalies in cloud environment based on the model of configurable activation threshold / N. A. Soloviev, N. A. Tishina, E. N. Chernoprudova // Science and education: fundamental principles, technology, innovations: materials of the International scientific conference devoted to the 60th anniversary of the Orenburg state University. – Orenburg: «University», 2015. P. 248–253.