Методы распределенных рассуждений в интеллектуальных системах ситуационной осведомленности об инцидентах в критической информационной инфраструктуре

А. В. Чернов[1], М. А. Бутакова[2], В. Д. Верескун[3]
Ростовский государственный университет путей сообщения
[1]a.v.chernov@ieee.org, [2]butakova@rgups.ru, [3]vvd@rgups.ru

Аннотация **Рассмотрен новый класс интеллектуальных систем ситуационной осведомленности, которые предназначены для принятия оперативных решений о возникновении и обработке инцидентов в критической информационной инфраструктуре. Рассмотрены особенности критической информационной инфраструктуры на примере комплекса информационных систем Российских железных дорог. Приведены возможные типы инцидентов, возникающих в критической информационной инфраструктуре. Сформулирована задача обнаружения новых типов инцидентов в критической информационной инфраструктуре. Предложены методы принятия решений о ситуационной осведомленности в критической информационной инфраструктуре на основе моделей распределенных рассуждений в условиях частично неопределенной информации.**

Ключевые слова: распределенные рассуждения, интеллектуальные системы, принятие решений, ситуационная осведомленность, критическая информационная инфраструктура

I. Введение

Информационно-управляющая инфраструктура государственной транспортной корпорации ОАО «РЖД» является крупнейшей корпоративной вычислительной сетевой системой, обеспечивающей технологические процессы транспортировки грузов и пассажиров по железной дороге. Многогранные проблемы обеспечения безопасности технологических процессов и информационной безопасности инфраструктуры ОАО «РЖД» были рассмотрены ранее в научных работах [1–4] отечественных исследователей, в том числе работах [5,6] авторов данной статьи. Очевидная критическая составляющая информационно-управляющей инфраструктуры ОАО «РЖД» с недавнего времени закреплена законодательным образом [7]. Показатели критериев значимости объектов критической информационной инфраструктуры включают социальную, экономическую, политическую, экологическую значимость, а также значимость для обеспечения обороны страны и правопорядка, безопасности государства. Указанные категории и сами критерии в полной мере относятся к информационной инфраструктуре железнодорожного транспорта.

Следует заметить, что в упомянутом выше законе основным содержанием является критичность информационной инфраструктуры к нарушениям информационной безопасности. Обычно к сфере информационной безопасности относятся мероприятия, которые направлены на противодействие целевым угрозам. Однако, для информационно-управляющих систем на железнодорожном транспорте особое значение имеют аспекты технологической безопасности, рассматриваемые в условиях возникновения непреднамеренных событий или действий, связанных с корректностью функционирования систем. Информационно-управляющая система, эксплуатируемая на железнодорожном транспорте, не должна допускать возникновения и развития инцидентов, связанных с угрозой жизнедеятельности и здоровью людей, ущербом имуществу и окружающей среде, экономике и обороноспособности страны. Таким образом, класс критичных информационно-управляющих систем на железнодорожном транспорте является весьма широким со всех точек зрения.

Использование подсистем мониторинга событий и возникновения инцидентов является обычной практикой для критических информационных инфраструктур. Информационная инфраструктура и возможности распределенной вычислительной среды управления транспортными технологическими процессами ОАО «РЖД» в настоящее время обеспечивают непрерывный мониторинг и регистрацию инцидентов различного вида. Для задач оперативного управления на разных уровнях иерархии требуются не столько данные об инцидентах, а осведомленность о текущем положении дел, об оперативной обстановке и ситуации в целом. Данные обстоятельства позволяют четко обозначить потребности критической информационной инфраструктуры в ситуационном управлении. Особую роль в ситуационном управлении играет не только идентификация, и регистрация различных событий, связанных с

Работа выполнена при финансовой поддержке РФФИ, проекты № 16-01-00597-а, 17-07-00620-а, 18-01-00402-а.

возникновением различных ситуаций, приводящих, или могущих привести в дальнейшем к развитию нештатных режимов функционирования систем, авариям, сбоям, поломкам оборудования, к развитиям угроз безопасности людей, грузов, катастрофическим последствиям для окружающей природы и тому подобное. Дальнейшая обработка инцидентов и принятие решений, совместно с прогнозированием относятся к актуальным и приоритетным задачам для критической информационной инфраструктуры железнодорожного транспорта.

Задачи, связанные с обработкой инцидентов в критической информационной инфраструктуре железнодорожного транспорта, ведутся в настоящее время ручным образом с применением средств вычислительной техники. Развитие технологий интеллектуального принятия решений, появление новых информационно-управляющих систем с интеллектуальными возможностями существенно расширяет класс критических информационных инфраструктур на железнодорожном транспорте. Является очевидным, что интеллектуальные системы на железнодорожном транспорте должны обеспечивать поддержку принятия решений, не противоречащих с обеспечением основных целей и задач функционирования всей транспортной системы.

В связи с необходимостью перехода на новые технологии и требованиями ситуационного управления в работе рассмотрен новый класс интеллектуальных систем ситуационной осведомленности, которые предназначены для принятия оперативных решений о возникновении и обработке инцидентов в критической информационной инфраструктуре на примере ОАО «РЖД». Важной особенностью предлагаемого класса интеллектуальных систем ситуационной осведомленности является возможность использования подходов и методов распределенных рассуждений для извлечения новых знаний об инцидентах, происходящих в критической информационной инфраструктуре. Работа структурирована следующим образом. Во втором разделе приведена информация об имеющихся на настоящее время научных исследованиях в выбранной области. Третий раздел содержит анализ особенностей критической информационной инфраструктуры на примере комплекса информационных систем ОАО «РЖД». Приведены возможные типы инцидентов, возникающих в критической информационной инфраструктуре. В четвертом разделе сформулирована задача обнаружения новых типов инцидентов в критической информационной инфраструктуре и предложены методы принятия решений о ситуационной осведомленности в критической информационной инфраструктуре на основе моделей распределенных рассуждений.

II. Предыдущие исследования

Тематика ситуационной осведомленности и ситуационного управления в интеллектуальных системах управления железнодорожным транспортом вызывает особый интерес для научных исследований, в связи с нарастающей потребностью создания ситуационных центров на транспорте. В основе любого анализа возникшей ситуации лежит процесс регистрации и обработки инцидентов.

В работе [8] предложен метод обнаружения инцидентов нарушения информационной безопасности на основе теории приближенных множеств. Основным применением указанного метода является многоуровневая интеллектуальная система управления на железнодорожном транспорте. Дальнейшее развитие вышеупомянутого метода можно найти в работе [9]. В ней дается классификация инцидентов сетевой информационной безопасности в интеллектуальной системе управления железнодорожным транспортом, а также рассматривается общий процесс обработки инцидента безопасности, принятый в системах, которые эксплуатируются ОАО «РЖД».

Работа [10] содержит гибридный подход к обнаружению новых типов инцидентов, который базируется на совместном использовании математического аппарата теории нечетких систем и приближенных множеств. В рассматриваемом подходе выделяются два этапа: 1) предварительная обработка данных мониторинга инцидентов, которая осуществляется фаззификацией; 2) определение наиболее значащих признаков инцидентов, осуществляемое разбиением множества на классы эквивалентности. На первом этапе используется псевдодополнение нечеткого множества в решетке Брауэра.

При проведении вычислительных экспериментов с данными об инцидентах на критической информационной инфраструктуре ОАО «РЖД» было установлено, что именно первый этап, препроцессинг данных об инцидентах занимает наибольшее время из-за высокой вычислительной сложности. Дальнейшие исследования позволили предложить усовершенствованный метод предварительной обработки [11] данных об инцидентах, адаптированный к использованию классификаторов на базе теории приближенных множеств. Архитектура мобильных смарт объектов, являющихся программно-аппаратными агентами, предназначенными для выполнения задач непрерывного мониторинга инцидентов предложены в [12]. Препроцессинг данных выполняется аппаратным ускорителем на основе FPGA модуля. Системная архитектура сервиса ситуационной осведомлённости, разработанная на основе методов, предложенных в работах [8–12] представлена в [13] для многоуровневой интеллектуальной системы управления железнодорожным транспортом.

В области распределенных рассуждений в системах искусственного интеллекта следует выделить ряд работ, которые можно отнести к основным исследованиям, давшим фундамент для развития остальных подходов и методов. Модель убеждений, желаний и намерений [14, 15] включает в себя элементы знаний о реальном мире, необходимые для информированности программируемого агента об окружающей среде. По сути, информированность агента можно рассматривать как одну из составляющих ситуационной осведомленности в

многоагентной системе. Разнородность предметных областей, и, естественно онтологических описаний в сложных системах потребовали усовершенствования математического аппарата дескрипционной логики [16] для описания методов интеграции множественных онтологий. Такой подход имеет название распределенная дескрипционная логика [17–19]. В разделе 4 будут использованы подходы распределенной дескрипционной логики, применительно к задачам обеспечения ситуационной осведомленности об инцидентах на критической информационной инфраструктуре.

III. Инциденты в критической информационной инфраструктуре

В настоящее время процесс управления инцидентами в критической информационной инфраструктуре ОАО «РЖД» является интерактивным частично автоматизированным процессом с ручным вводом данных [20]. Он содержит следующие процедуры: «Регистрация Инцидента», «Решение Инцидента», «Закрытие Инцидента» «Контроль Инцидента», «Формирование отчётности», «Оценка и совершенствование процесса». Основанием для регистрации инфраструктурного инцидента является любое событие в обслуживаемой критической информационной инфраструктуре, которое привело к сбою или отказу программно-технических комплексов, оборудования или каналов сети передачи данных, инженерных систем в зоне ответственности Главного вычислительного центра ОАО «РЖД», повлиявшее на качество предоставления сервисов. По обращениям, классифицируемым как «Инцидент», диспетчерский персонал создает инциденты и назначает в рабочие группы согласно листам маршрутизации.

Приведем примеры инцидентов, описываемых в общем случае разными онтологиями, однако, имеющими сходную семантику. Примерами инцидентов, возникающих на рабочих местах пользователей, являются следующие обращения пользователей: 1) не включается компьютер; 2) наблюдаются сбои компьютера; 3) не работает какая-либо функция программного обеспечения; 4) ошибка в работе автоматизированного рабочего места; 5) не работает транзакционный терминал самообслуживания, билетно-кассовое оборудование, электронный терминал самообслуживания; 6) не работает/не печатает принтер; 7) отсутствует сетевое соединение автоматизированного рабочего места. Примерами инфраструктурных инцидентов в *IT*-сервисах являются следующие события: 1) недоступность оборудования сети передачи данных в мониторинге; 2) отказ или сбой оборудования сети передачи данных; 3) отказ или сбой серверного оборудования; 4) отказ или сбой сервера приложений; 4) остановка процесса, сервиса или службы на сервере; 5) сбой в работе программно-прикладного обеспечения; 6) неработоспособность части функционала программного обеспечения; 7) массовые (более 3-х) обращения пользователей по одному событию; 8) недоступность ссылки для конкретного *IT*-сервиса. Заметим, что в приведенных примерах, как для автоматизированных рабочих мест, так и для инфраструктурных инцидентов во всей *IT*-инфраструктуре имеются семантически сходные инциденты. Тем не менее при ручном вводе имеются значительные различия в их формулировке.

Сформулируем основную задачу исследования об обнаружении нового типа инцидентов в критической информационной инфраструктуре. Пусть даны исходные онтологии предметных областей и имеется схема генерации нового типа инцидента. Требуется при обнаружении нового типа инцидента выполнить интеграцию онтологий для обобщённого семантического представления информации, сформировать некоторую общую онтологию из частных и обеспечить тезаурус функционирования системы ситуационной осведомленности. Для того, чтобы использовать автоматизированные подходы к принятию решений в интеллектуальных системах ситуационной осведомленности в следующем разделе предлагается методы распределенных рассуждений, построенные на основе расширений распределенной дескрипционной логики.

IV. Предлагаемый подход

Ситуационная осведомленность подразумевает возможность получения полной и достоверной информации для принятия решений в режиме реального времени, включая характеристики и особенности ситуации. Ситуационная осведомленность представляет собой трёхступенчатый процесс [21]: 1) восприятие элементов окружающей среды; 2) понимание текущей ситуации; 3) прогноз будущего состояния. По аналогии с этим, первым этапом предлагаемого подхода является составление классификаторов предметных областей. На рис. 1 показан трехступенчатый процесс для классификаторов системы ситуационной осведомленности критической информационной инфраструктуры.

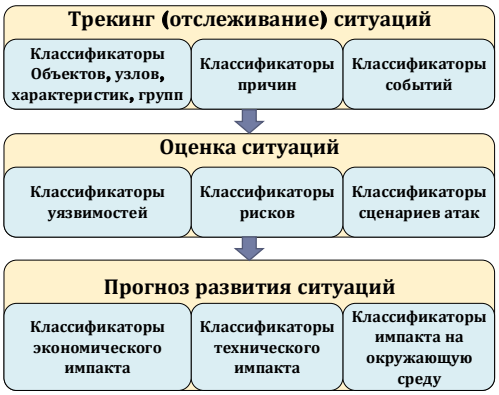

Рис. 1. Процесс создания классификаторов

На втором этапе дается формальное определение распределенной базы знаний. В терминах работы [22] эта формализация выглядит следующим образом. Распределенная база знаний D об инцидентах состоит из двух частей: 1) терминологии *TBox* и 2) утверждений *ABox*. Определим $D = \left(T, \bigcup_j A_j \right)$, где T – это *TBox*, A_j –

это $ABox$, $1 \le j \le n$. Части базы распределенной базы знаний D обозначим K_j, $1 \le j \le n$. Интерпретацию I назовем моделью $T(I|=T)$, если она удовлетворяет всем аксиомам в T или моделью $A(I|=A)$, если удовлетворяет всем утверждениям в A.

Наконец, на третьем этапе формулируется распределенная система рассуждений R для распределенной базы знаний D. Система рассуждений состоит из n программных агентов R_j, принимающих решения, $1 \le j \le n$. Каждый программный агент ассоциирован с отдельной частью K_j базы знаний. При этом должны быть обеспечены требования непротиворечивости знаний. Очевидным является факт, что если K_j непротиворечива для $\forall j$, то распределенная база знаний D также является непротиворечивой.

V. Выводы

В работе обоснована необходимость разработки новых методов автоматизации обнаружения инцидентов для критической информационной инфраструктуры железнодорожного транспорта. Наиболее современным и перспективным способом для решения поставленной задачи является создание систем ситуационной осведомленности в рамках разрабатываемых интеллектуальных систем управления железнодорожным транспортом. На основе имеющегося опыта разработки систем обнаружения инцидентов нарушения информационной безопасности в транспортных системах авторы предлагают использование распределенных методов рассуждений для интегрированных онтологий предметных областей.

Список литературы

[1] Шматченко В.В., Плеханов П.А. Управление безопасностью высокоскоростного железнодорожного транспорта // Бюллетень результатов научных исследований. 2017. №3. С. 105-118.

[2] Ульянов В.А. Оценка уровня технологической безопасности на железнодорожном транспорте // Наука и техника транспорта. 2015. №2. С. 8-15.

[3] Розенберг Е.Н., Батраев В.В. Разработка перспективных систем управления и обеспечения безопасности движения поездов // Бюллетень объединенного ученого совета ОАО «РЖД». 2017. №4. С. 43-51.

[4] Котенко И.В., Саенко И.Б. Предложения по созданию многоуровневой интеллектуальной системы обеспечения информационной безопасности автоматизированных систем на железнодорожном транспорте // Вестник Ростовского государственного университета путей сообщения. 2013. № 3(51). С. 69-79.

[5] Бутакова М.А., Гуда А.Н., Гнаденберг В.С. Методы оценки надежности и технологической безопасности управляющего программного обеспечения автоматизированных систем управления на железнодорожном транспорте // Вестник Ростовского государственного университета путей сообщения. 2011. №3(43). С. 22-32.

[6] Котенко И.В., Саенко И.Б., Чернов А.В., Бутакова М.А. Построение многоуровневой интеллектуальной системы обеспечения информационной безопасности для автоматизированных систем железнодорожного транспорта // Труды СПИИРАН. 2013. №7(30). С. 7-25.

[7] «О безопасности критической информационной инфраструктуры Российской Федерации». Федеральный закон №187-ФЗ от 26.07.2017 г.

[8] Chernov A.V., Butakova M.A., Karpenko E.V. Security incident detection technique for multilevel intelligent control systems on railway transport in Russia // 23rd Telecommunications Forum TELFOR. 2015. pp. 1-4. doi: 10.1109/TELFOR.2015.7377381

[9] Chernov A.V., Butakova M.A., Karpenko E.V., Kartashov O.O. Improving Security Incidents Detection for Networked Multilevel Intelligent Control Systems in Railway Transport // Telfor Journal. 2016. v.8, №1. pp. 14-19. doi:10.5937/telfor1601014C

[10] Chernov A.V., Bogachev V.A., Karpenko E.V., Butakova M.A., Davidov, Y.V. Rough and fuzzy sets approach for incident identification in railway infrastructure management system // Proceedings of the 19th International Conference on Soft Computing and Measurements, SCM. 2016. pp. 228-230. doi: 10.1109/SCM.2016.7519736

[11] Chernov A.V., Kartashov O.O., Butakova M.A., Karpenko E.V. Incident data preprocessing in railway control systems using a rough-set-based approach // Proceedings of the 20th IEEE International Conference on Soft Computing and Measurements, SCM. 2017. pp. 248-251. doi: 10.1109/SCM.2017.7970551

[12] Chernov A.V., Butakova M.A., Vereskun V.D., Kartashov O.O. Mobile smart objects for incidents analysis in railway intelligent control system // Advances in Intelligent Systems and Computing. 2017. v. 680. pp. 128-137. doi: 10.1007/978-3-319-68324-9_14

[13] Chernov A.V., Butakova M.A., Vereskun V.D., Kartashov O.O. Situation awareness service based on mobile platforms for multilevel intelligent control system in railway transport // 24th Telecommunications Forum, TELFOR. 2016. pp. 1-4. doi:10.1109/TELFOR.2016.7818714

[14] Georgeff M., Pell B., Pollack M., Tambe M., Wooldridge M. The Belief-Desire-Intention Model of Agency. // Intelligent Agents V: Agents Theories, Architectures, and Languages. Lecture Notes in Computer Science. 1999. v. 1555. pp. 1-10. doi: 10.1007/3-540-49057-4_1

[15] Rao A.S., Georgeff M.P. BDI agents: From theory to practice // Proceedings of the First International Conference on Multiagent Systems. 1995. pp. 312-319.

[16] Baader F., Calvanese D., McGuinness D., Nardi D., Patel-Schneider P.F., editors.The Description Logic Handbook: Theory, Implementation and Applications, 2nd Edition. Cambridge University Press. 2010. 624p.

[17] Borgida A., Serafini L. Distributed Description Logics: Assimilating Information from Peer Sources. // Journal on Data Semantics I. Lecture Notes in Computer Science. 2003 v. 2800. pp. 153-184. doi: 10.1007/978-3-540-39733-5_7

[18] Serafini L., Tamilin A. Local tableaux for reasoning in distributed description logics. // Proceedings. of DL'04. CEUR-WS. 2004. URL: http://ceur-ws.org/Vol-104/12Serafini-final.pdf

[19] Serafini L., Borgida A., Tamilin A. Aspects of distributed and modular ontology reasoning. // Proceedings. of IJCAI'05. 2005. URL: http://www.ijcai.org/Proceedings/05/Papers/0801.pdf

[20] Vereskun V.D., Butakova M.A., Ivanchenko O.V. An approach to interactive information processing for situation awareness about incidents in railway infrastructure management system // Advances in Intelligent Systems and Computing. 2016. v. 451, pp. 313-322. doi: 10.1007/978-3-319-33816-3_31

[21] Endsley M.R., Garland D. G. Situation awareness analysis and measurement. CRC Press. 2000. 408 p.

[22] Horrocks I., Sattler U., Tobies S. Reasoning with Individuals for the Description Logic SHIQ // Proceedings of 17th International Conference on Automated Deduction (CADE). 2000. pp. 482-496.