УДК 004.89

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ИНТЕЛЛЕКТУАЛЬНЫХ СЕМАНТИЧЕСКИХ СИСТЕМАХ

канд. техн. наук, доц. В. М. ЧЕРТКОВ

(Полоцкий государственный университет имении Евфросинии Полоцкой)

Развитие искусственного интеллекта обуславливает переход на семантические технологии обработки информации, которые требует формирование новых подходов к обеспечению информационной безопасности таких систем. Статья посвящена обзору подходов и принципов обеспечения безопасности в интеллектуальных системах нового поколения. Приводиться современное состояние обеспечения информационной безопасности в интеллектуальных системах и представлены сформированные основные цели и направления по развитию обеспечения информационной безопасности. Рассмотренные в статье методы обеспечения безопасности информации являются чрезвычайно важными при анализе уровня защищённости интеллектуальных систем нового поколения.

Ключевые слова: *информационная безопасность, интеллектуальные системы, семантические системы.*

Введение. Одним из современных направлений развития информационных технологий является переход к работе с семантикой информации и создание интеллектуальных систем нового поколения [1]. Основным преимуществом которых является организованная работа с семантической базой знаний. Особенностью такой базы знания является то, интеллектуальная система способна получить новые знания, которые непосредственно в базе не содержатся.

Так как проектирование, построение и использование интеллектуальных систем основанных на семантических базах знаний начались относительно недавно, то вопрос обеспечения их безопасности решен ещё не в полной мере. В связи с этим актуальным является разработка методов и алгоритмов, позволяющих поддерживать безопасность функционирования таких интеллектуальных систем.

Следует отметить, что искусственный интеллект (машинное обучение) активно применяется для мониторинга и анализа уязвимостей безопасности в сетях передачи информации [2]. В работе [3] предложена методика построения нейроиммунной системы анализа инцидентов информационной безопасности, объединяющей модули сбора и хранения (сжатия) данных, модуль анализа и корреляции событий информационной безопасности и подсистемы обнаружения сетевых атак на основе сверточных нейронных сетях. Использование технологий машинного

обучения в информационной безопасности создает узкие места и системные уязвимости, которые можно использовать и имеет следующие недостатки [4]:

– наборы данных, которые должны быть сформированы из значительного количества входных выборок, что требует много времени и ресурсов;

– требуется огромное количество ресурсов, включая память, данные и вычислительную мощность;

– частые ложные срабатывания, которые нарушают работу и в целом снижают эффективность таких систем;

– организованные атаки на основе искусственного интеллекта (семантические вирусы).

Исходя из вышеизложенного определим цели обеспечения информационной безопасности систем нового поколения.

Из монографии А. В. Остроух [5] ***целями обеспечения информационной безопасности традиционных интеллектуальных систем*** являются обеспечение сохранности и конфиденциальности информации, защита и гарантия доступности, достоверности и целостности информации, избежание утечки информации, минимизация ущерба от событий, несущих угрозу информационной безопасности.

Следует отметить так как интеллектуальные системы нового поколения будет взаимодействовать с подобными себе системами понимая при этом, о чем осуществляется запрос, то цели обеспечения будет выглядеть по-другому. ***Целями обеспечения информационной безопасности интеллектуальных систем нового поколения***: являются обеспечение сохранности семантической совместимости информации, защита достоверности и целостности информации, обеспечение доступности информации на разных уровнях интеллектуальной системы, минимизация ущерба от событий, несущих угрозу информационной безопасности.

В настоящее время разработаны классические подходы и принципы обеспечения безопасности баз знаний (данных), интерфейсов связи (обмена информацией) между компонентами интеллектуальных систем такие, как шифрование передаваемых данных, фильтрация ненужного (избыточного) контента и политика разграничения доступа к данным.

Для интеллектуальных систем нового поколения можно выделить основные направления, в рамках которых требуется работка новых алгоритмов и методов обеспечения информационной безопасности:

Ограничение информационного трафика, анализируемого интеллектуальной системой

Экспоненциальный рост объема информации, циркулирующей в информационных патоках и ресурсах в условиях вполне определенных количественных ограничений на возможности средств ее восприятия, хранения, передачи и преобразования формирует новый класс угроз информационной безопасности,

характеризуемых избыточностью совокупного входящего информационного трафика интеллектуальных систем.

В результате переполнение информационных ресурсов интеллектуальной системы избыточной информацией может спровоцировать распространения искаженной (деструктивной семантической) информации. Общая методология защиты интеллектуальных систем от бесполезной информации осуществляется посредством использования аксиологических фильтров, реализующих функции численной оценки ценности поступающей информации, отбора наиболее ценной и отсеивания (фильтрации) менее ценной (бесполезной или вредной) с использованием вполне определенных критериев.

Следует также выделить в отдельную категорию угроз информационной безопасности активные средства разрушения семантики баз знаний (семантические вирусы) [6].

Политика разграничении доступа к базе знаний

Мандатная политика безопасности (MAC – mandatory access control) основывается на мандатном (принудительном) разграничении доступа, определяющемся четырьмя условиями: все субъекты и объекты системы идентифицируются; задается решетка уровней безопасности информации; каждому объекту системы присваивается уровень безопасности, определяющий важность содержащейся в нем информации; каждому субъекту системы присваивается уровень доступа, определяющий уровень доверия к нему в интеллектуальной системе. Кроме того, мандатная политика имеет более высокую степень надёжности. Реализация данной политики основывается на разработанном алгоритме определения согласованных уровней безопасности всех элементов онтологии.

Так как семантические базы знаний в отличие от реляционной базы данных позволяют выполнять правила для получения логических выводов, то для обеспечения безопасности данных актуальным является разработка алгоритмов и методов, с помощью которых можно будет получать только данные, имеющие уровни безопасности меньше уровней доступа субъектов их запросивших [7].

Связность

Вся информация, хранимая в памяти компьютерной системы, систематизирована в виде единой базы знаний. К такой информации относятся непосредственно обрабатываемые знания, интерпретируемые программы, формулировки решаемых задач, планы и протоколы решения задач, информация о пользователях, описание синтаксиса и семантики внешних языков, описание пользовательского интерфейса и многое другое [8]. В информационной базе знаний между фрагментами информации (единицами информации) должна быть предусмотрена возможность установления связей различного типа. Прежде всего, эти связи могут характеризовать отношения между информационными единицами. Нарушение связей приводит к неправильному логическому выводу, либо к получению ложных знаний, либо к несовместимости знаниям в базе.

Семантическая метрика

На множестве информационных единиц в некоторых случаях полезно задавать отношение, характеризующее ситуационную близость информационных единиц, т. е. силу ассоциативной связи между информационными единицами. Его можно было бы назвать отношением релевантности для информационных единиц. Такое отношение дает возможность выделять в информационной базе знаний некоторые типовые ситуации. Отношение релевантности при работе с информационными единицами позволяет находить знания, близкие к уже найденным.

Семантическая совместимость

Внутренняя семантическая совместимость между компонентами интеллектуальной компьютерной системы (т. е. максимально возможное введение общих, совпадающих понятий для различных фрагментов хранимой базы знаний), являющаяся формой конвергенции и глубокой интеграции внутри интеллектуальной компьютерной системы для различного вида знаний и различных моделей решения задач, что обеспечивает эффективную реализацию мультимодальности интеллектуальной компьютерной системы. Внешняя семантическая совместимость между различными интеллектуальными компьютерными системами, выражающаяся не только в общности используемых понятий, но и в общности базовых знаний и являющаяся необходимым условием обеспечения высокого уровня социализации интеллектуальных компьютерных систем [9].

Активность

В интеллектуальной системе для актуализации тех или иных действий способствуют знания, имеющиеся в этой системе. Таким образом, выполнение активностей в интеллектуальной системе должно инициироваться текущим состоянием информационной базы знаний. Появление в базе фактов или описаний событий, установление связей может стать источником активности системы. В том числе преднамеренное искажение информации и связей может стать источником преднамеренное искажения информации.

Заключение. В настоящее время не существует баз знаний, в которых в полной мере были бы реализованы внутренняя интерпретируемость, структуризация, связность, введена семантическая мера и обеспечена активность знаний. Рассмотренные в статье методы обеспечения безопасности информации являются чрезвычайно важными при анализе уровня защищённости интеллектуальных систем нового поколения.

ЛИТЕРАТУРА

1. Семантические технологии проектирования интеллектуальных систем и семантические ассоциативные компьютеры / В. В. Голенков [и др.] // Доклады Белорусского Государственного Университета Информатики И Радиоэлектроники. – 2019. – № 3 (121). – С. 42–50.
2. Исобоев, Ш.И. Интеллектуальная система мониторинга безопасности сети беспроводной связи на основе машинного обучения / Ш. И. Исобоев, Д. А. Везарко, А. С. Чечельницкий // Экономика и качество систем связи, № 1(23). – 2022. – С. 44–48.

3. Частикова, В. А. Методика построения системы анализа инцидентов информационной безопасности на основе нейроиммунного подхода / В. А. Частикова, А. И. Митюгов // Электронный Сетевой Политематический Журнал «Научные Труды Кубгту». – 2022. – № 1. – С. 98–105.
4. Абдурахман, Д. Д. Искусственный интеллект и машинное обучение в кибербезопасности / Д. Д. Абдурахман // Современные проблемы лингвистики и методики преподавания русского языка в вузе и школе. – 2022. – № 34. – С. 916–921.
5. Остроух, А. В. Интеллектуальные системы: монография / А. В. Остроух. – Красноярск : Научно-инновационный центр, 2020. – 316 с.
6. Баранович, А. Е. Семантические аспекты информационной безопасности: концентрация знаний / А. Е. Баранович // История и архивы. – 2011.– № 13 (75). – С. 38–58.
7. Хоанг, К. В. Решения основных задач в разработке программы поддержки безопасности работы с семантическими базами данных / К. В. Хоанг, А. Ф. Тузовский // Доклады ТУСУРа. – 2013. – № 2 (28), С. 121–125.
8. Семантическая модель представления и обработки баз знаний / В. В. Голенков [и др.] // Федеральный исследовательский центр «Информатика и управление» Российской академии наук. – 2017. – С. 412–419.
9. Голенков, В. В. Текущее состояние и направления развития технологий искусственного интеллекта / В. В. Голенков, Н. А. Гулякина, Д. В. Шункевич // Информационные технологии и системы 2018 (ИТС 2018) = Information Technologies and Systems 2018 (ITS 2018) : материалы международной научной конференции, Минск, 25 октября 2018 г. / Белорусский государственный университет информатики и радиоэлектроники ; редкол. : Л. Ю. Шилин [и др.]. – Минск, 2018. – С. 11–16.