УДК 004.89

ОБЪЕДИНЕНИЕ СИСТЕМ РАСПРЕДЕЛЕННОГО РЕЕСТРА И МАШИННОГО ФЕДЕРАЛЬНОГО ОБУЧЕНИЯ

А.М. Макаров, Е.А. Писаренко, И.Н. Кутовой, Б.М. Гаджимуратов
ФГБОУ ВО «Пятигорский государственный университет»,
г. Пятигорск, Российская Федерация.

Аннотация. В работе рассматривается решение задачи целостности обучающих данных искусственного интеллекта на основе объединения систем с распределенным реестром (блокчейн), и технологий криптографии в системах федерального обучения искусственного интеллекта. При этом обеспечивается конфиденциальности данных, защите их от фальсификации, модификации и уничтожения является в настоящее время важной задачей производства систем с ИИ. Рассмотрена целесообразность отдельного включения временных меток в протоколы нотариуса-криптографа. Далее приводятся схема блок- структур, объединяющие технологии обучения и технологии информационной безопасности режима федерального обучения ИИ.
Ключевые слова: искусственный интеллект; федеральное обучение; временные метки; блокчейн технология; криптография; хэширование.

COMBINING DISTRIBUTED LEDGER SYSTEMS AND MACHINE FEDERAL LEARNING

A.M. Makarov, E.A. Pisarenko, I.N. Kutovoy, B.M. Gadzhimuratov
Federal State Budgetary Educational Institution of Higher Education
"Pyatigorsk State University",
Pyatigorsk, Russian Federation.

Annotation. The paper deals with the solution of the problem of integrity of artificial intelligence training data on the basis of combining systems with distributed registry (blockchain), and cryptography technologies in the systems of federal training of artificial intelligence. At the same time the confidentiality of data, protection of data from falsification, modification and destruction is currently an important task of production of systems with AI. The feasibility of separate inclusion of timestamps in notary cryptographer protocols is considered. Further, the scheme of blockchain structures combining training technologies and information security technologies of the federal AI training mode is given.
Keywords: Artificial Intelligence; federal learning; timestamps; blockchain technology; cryptography; hashing.

Введение

Внедрение генеративного искусственного интеллекта (ИИ) в практику обучающих, справочных и типовых текстов привело к необходимости разработки государственных стандартов, регламентов, а также юридических правил использования ИИ, как в обществе, так и в сферах, где требуется выполнение определенных правил этики поведения феномена ИИ. Следует заметить, что первые угрозы возникают на этапах обучения, дообучения и переобучения памяти ИИ. Особенно остро стоит задача по использованию достоверных обучающих данных, а также их надежного хранения непосредственно в самой системе ИИ.

Сохранение конфиденциальности данных, защите их от фальсификации, модификации и уничтожения является в настоящее время важной задачей производства систем с ИИ. Таким образом, весьма актуально решение вышеперечисленных задач в плане обеспечения информационной безопасности данных во всей их разнообразии палитр.

Материалы и методы

Проникновение новых технологий в системы с распределенным реестром, реализованных на блокчейн технологии, в основе которой лежат методы криптографии, происходит во все сферы социально-экономической деятельности общества. Императивный стиль в проектировании социально-экономических систем это такой, при котором предварительно выработанные заранее требования (аксиомы) к их свойствам, должен непременно выполняться проектировщиком, для достижения технических и социально-экономических целей (1, 2, 3).

Для решения задачи сформулируем пять императивных требования:

1. Наличие абонентов, объединенных решаемой задачей, которым система с распределенным реестром необходима для доверительной работы абонентов, не доверяющих друг другу. И, как следствие, отсутствие централизованного контроля сети. Все абоненты сети являются контролерами их работы с правом вмешаться в любой момент времени в любой точке цепи работы.

2. Обязательное формирование всей базы данных всех транзакций в сети распределенного реестра абонентов и обязательное обеспечение каждого абонента всеми текущими блоками транзакций в реальном масштабе времени.

3. Абоненты сети не являются профессиональными криптографами. Эту роль играет профессиональный нотариус-криптограф. Это новая роль майнера, требующая своего развития.

4. Формируемая база транзакций, всегда должна быть одноранговой цепью, включающая все блоки, включенные в сеть (ошибочные, испорченные, по ошибке включенные и так далее). Без права уничтожать, заменять, корректировать данные включенных блоков, вставлять, шунтировать блоки и так далее.

5. Все, перечисленные выше требования к системам распределенного реестра (блокчейн технология), погружаются в «океан» криптографического шифрования и криптографических технологий.

Результаты

Схема федерального централизованного обучения не требует загрузки данных абонентов, участвующих в дообучении ИИ. Это позволило решить задачу сохранения конфиденциальности персональных данных абонентов.

На рис. 1 представлена структура, использующая технологию блокчейн. В качестве абонентов, объединенных общей задачей обучения, служат различные носители обучающих данных (ТАА и ДО). Они образуют систему распределенного реестра с заинтересованными лицами, каждый из которых имеет свой уникальный цифровой токен и цифровую подпись. Посредством нотариуса-криптографа блоки с обучающими данными встраиваются в одноранговую цепь и рассылают общую базу данных серверов каждого абонента в системе распределенного реестра. На рис. 1 приведена система распределенного реестра (блокчейн технология), в которую встроена система ИИ. В данном случае кибербезопасность ИИ полностью защищена блокчейн технологией. Причем в качестве достоверности и целостности данных используется стрела меток времени прикрепления каждого блока в одноранговую сеть. Вторым видом федерального обучения называемого совместным в их ИИ обучается на множестве децентрализованных абонентов или серверов. То есть обучающие данные

не загружаются в общий сервер и не являются одинаково распределенными данными каждого абонента, участвующего в обучении.

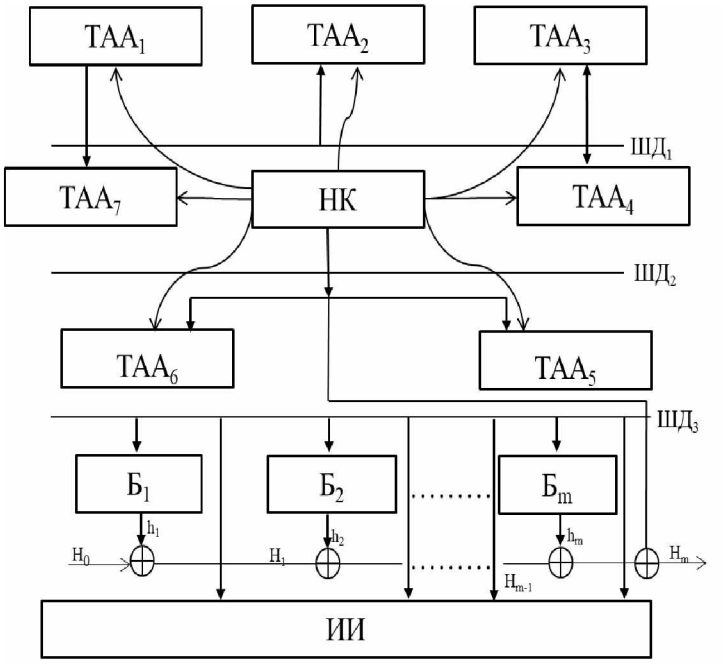

Рис. 1 Структура, использующая технологию блокчейн в федеральном способе обучения
Fig. 1 Structure utilizing blockchain technology in the federal way of learning

Сформулированные в работе императивные требования позволили оценить возможность применения технологии блокчейн для построения единой системы искусственного интеллекта с одновременным обеспечением информационной безопасностью целостности обучающих данных. Применение технологии временных меток для формирования вторых хешей блоков основной сети позволило упростить контроль свежести времени встраивания блоков блокчейн в основную одноранговую цепь для абонентов сети. Эти результаты показывают эффективность и целесообразность встраивания технологии распределенного реестра в общую систему обучения. Но в тоже время остался открытым вопрос, количественной экономической оценки стоимости и киберстойкости всей системы в целом. Эти две отмеченные задачи требуют дополнительного исследования и анализа.

Список использованных источников

1. Судас Л.Г. Управленческие императивы Индустрии 4.0 / Л.Г. Судас, М.А. Юдина. – М. : Издательство Московского университета, 2021. – 152 с. – (Библиотека факультета государственного управления МГУ. Научные исследования, электронное издание сетевого распространения).

2. Что такое императивное управление процессами. URL: https://totallsocks.ru/chto-takoe-imperativnoe-upravlenie-protsessami.

3. Макаров А.М., Писаренко Е.А. Перспективы развития теории систем распределенного реестра в управлении социальноэкономическими объектами. В сборнике: Инновационные тренды в международном бизнесе и устойчивом менеджменте. Материалы II Международной научно-практической конференции. Новокузнецк, 2023. С. 221-232.

References

1. Sudas, L.G. Upravlenie imperatives of Industry 4.0 / L. G. Sudas. M. A. Yudina. – Moscow: Moscow University Press, 2021. – 152 p. (Library of the Faculty of Public Administration of Moscow State University. Scientific research, electronic edition of network distribution).

2. What is imperative process management. URL: https://totallsocks.ru/chto-takoe-imperativnoe-upravlenie-protsessami.

3. Makarov A.M., Pisarenko E.A. PERSPECTIVES OF DEVELOPMENT OF THEORY OF DISPLACED LISTING SYSTEMS IN MANAGEMENT OF SOCIAL ECONOMIC OBJECTS. In collection: Innovative trends in international business and sustainable management. Materials of the II International Scientific and Practical Conference. Novokuznetsk, 2023. C. 221-232.

Сведения об авторах

Макаров А.М., д-р техн. наук, проф., проф. каф. информационно-коммуникационных технологий, математики и информационной безопасности, Пятигорский государственный университет, e-mail mellin_22@mail.ru.
Писаренко Е.А., канд. пед. наук, доц., доц. каф. информационно-коммуникационных технологий, математики и информационной безопасности, Пятигорский государственный университет, e-mail elt@yandex.ru.
Кутовой И.Н., канд. пед. наук, доц., доц. каф. информационно-коммуникационных технологий, математики и информационной безопасности, Пятигорский государственный университет, e-mail igor196428@yandex.ru.
Гаджимурадов Б.М., канд. экон. наук, ст. преп. каф. информационно-коммуникационных технологий, математики и информационной безопасности, Пятигорский государственный университет, e-mail baxa78@bk.ru.

Information about the authors

Makarov A.M., D.Sc. (Eng.), Prof., Prof., Dept. of Information and Communication Technologies, Mathematics and Information Security, Pyatigorsk State University, e-mail mellin_22@mail.ru.
Pisarenko E.A., Ph.D. (Ped.), Assoc. Prof., Dept. of Information and Communication Technologies, Mathematics and Information Security, Pyatigorsk State University, e-mail elt@yandex.ru.
Kutovoy I.N., Ph.D. (Ped.), Assoc. Prof., Dept. of Information and Communication Technologies, Mathematics and Information Security, Pyatigorsk State University, e-mail igor196428@yandex.ru
Gadzhimuradov B.M., Ph.D. (Econ.), Senior Lecturer, Dept. information and communication technologies, mathematics and information security, Pyatigorsk State University, e-mail baxa78@bk.ru