ORES

Научно-практический электронный журнал
Оригинальные исследования (ОРИС), *ISSN 2222-0402*
www.ores.su
original-research.ru

ПРИМЕНЕНИЕ МЕТОДОВ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ ПОВЫШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УНИВЕРСИТЕТАХ

Пензин Антон Олегович,
аспирант, Тюменский индустриальный университет
Россия, г. Тюмень
E-mail: Anton_toshiba@mail.ru

Аннотация

Высокий уровень безопасности данных необходим во многих областях образования. В данном исследовании представлен обзор литературы по вопросам безопасности данных и конфиденциальности в университетах. Рассмотрены и проанализированы различные методы искусственного интеллекта, их роль в обеспечении защиты данных. В заключительной части работы представлены различные методы повышения безопасности и конфиденциальности данных. Могут быть использованы две структуры, основанные на подходах искусственного интеллекта, обрабатывающие атаки с входными данными в виде текстов или биометрической информации.

Ключевые слова: безопасность данных, искусственный интеллект, конфиденциальность данных, утечки данных

APPLICATION OF ARTIFICIAL INTELLIGENCE METHODS TO ENHANCE INFORMATION SECURITY IN UNIVERSITIES

Anton O. Penzin,
postgraduate student, Industrial University of Tyumen
Russia, Tyumen
E-mail: Anton_toshiba@mail.ru

ABSTRACT

High level of data security is needed in many fields of educational areas. In this research, a literature review of data security and privacy in universities is provided, many Artificial intelligence methods are explained and explored by their roles in the field of data security. Some different methods of enhancement data security and privacy are also provided at the end, two structures can be used based on Artificial Intelligence approaches that handle attacks with input of form texts or biometrics data.

Keywords: data security, artificial intelligence, data privacy, data breaches

Вопрос обеспечения безопасности, конфиденциальности и защиты данных в университетах занимает важное место в современном мире, поскольку численность и масштабы киберпреступлений увеличиваются с каждым днём. Обеспечение безопасности данных в университетах имеет важное значение для студентов, сотрудников и преподавателей. Например, сохранность данных экзаменов играет ключевую роль в организации и совершенствовании образовательного процесса. В условиях роста числа кибератак и киберпреступлений возникает необходимость усиления мер по защите данных. Искусственный интеллект может быть использован в качестве инструмента, способствующего обеспечению информационной безопасности в университетской среде 1. В январе 2023 г. исследование, проведенное в Китае, представило результаты анализа актуальных киберугроз в университетах Китая. Анализ показал, что число кибератак в январе 2023 года выросло на 300% по сравнению с 2021 годом (рисунки 1) [1]. В России количество атак на данные в целом увеличилось на 54 % [2].

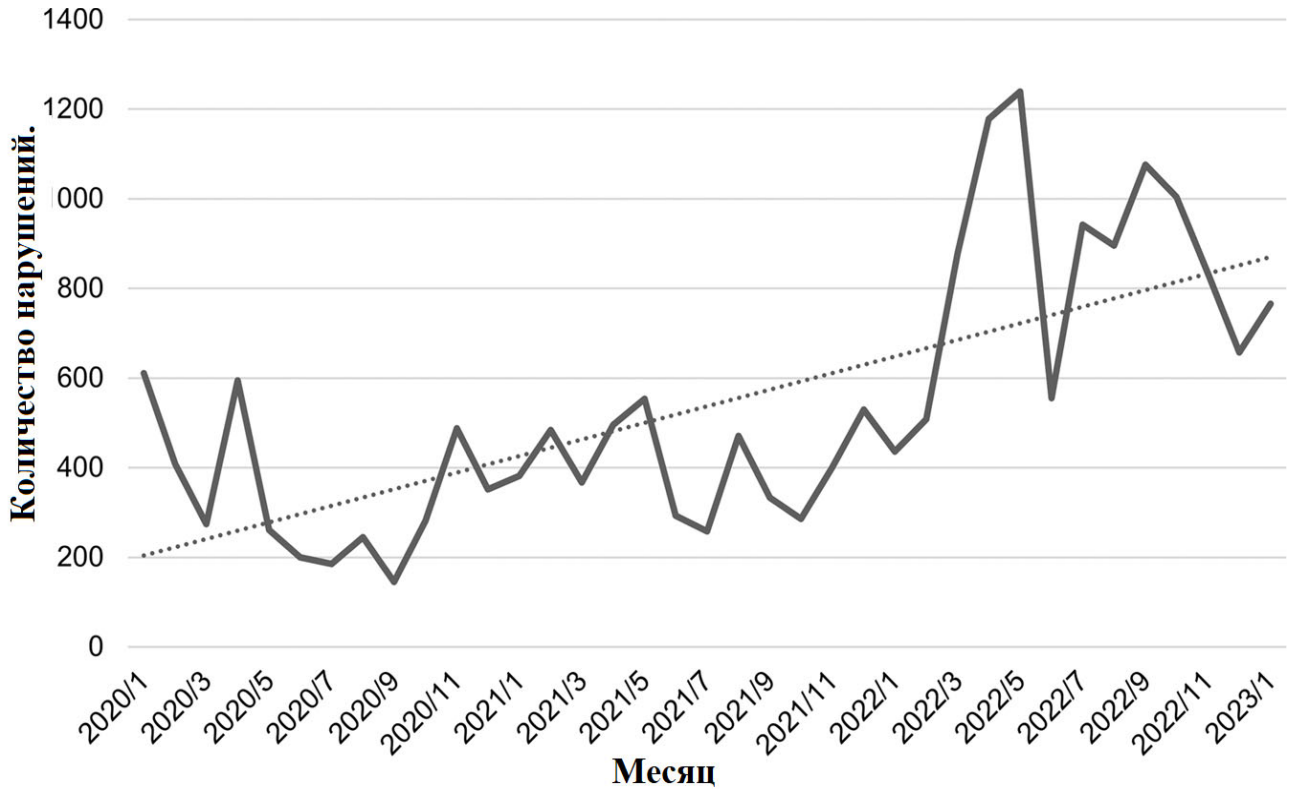

Рисунок 1 - Ежемесячно увеличивается количество утечек данных [2]

Целью данного исследования является изучение современных методов искусственного интеллекта, используемых для защиты безопасности и конфиденциальности университетских данных.

В научной литературе активно изучается влияние генеративно-состязательных сетей (Generative Adversarial Networks, GAN) на защиту данных от кибератак [3].

В исследовании [4] рассматривается важность критического переосмысления ряда допущений, связанных с аналитикой обучения, в контексте взаимосвязи между данными студентов и институциональной подотчётностью, а также более широких вопросов, касающихся масштабов и последствий практик цифрового надзора. Авторы анализируют распространённые предположения о потенциале больших данных в системе высшего образования — например, что сами по себе большие данные обеспечивают большую точность и объективность, что наблюдение осуществляется исключительно в одном направлении, а также что доступные данные представляют собой целостную картину учебной деятельности студентов.

В данном исследовании представлена структура подхода, основанного на применении методов искусственного интеллекта для повышения уровня безопасности данных в университетах. Для более глубокого понимания предлагаемого метода необходимо принять ряд допущений: предполагается наличие набора данных, содержащего запросы или обращения с метками, указывающими на их безопасность (безопасный / небезопасный), который используется для обучения модели ИИ [5].

Ключевым аспектом является то, что любая модель искусственного интеллекта в данном контексте является локальной, то есть для каждого университета разрабатывается уникальная модель, отличающаяся от моделей, используемых в других учреждениях.

Основные этапы предлагаемого подхода по защите данных следующие:

Злоумышленник использует текстовые данные для осуществления атаки — это может быть веб-ссылка, скрипт, кнопка (с гиперссылкой в фоновом режиме), электронное письмо от неизвестного отправителя и т.п.

Независимо от формы атаки, текстовое содержимое должно быть проанализировано с применением методов обработки естественного языка (Natural Language Processing, NLP).

После анализа текста из него извлекаются признаки, которые затем подаются на вход предварительно обученной модели, прошедшей обучение на датасете, содержащем как безопасные, так и аномальные запросы.

Предварительно обученная модель принимает решение о том, является ли данный запрос безопасным или нет.

Простая структура этой комбинации показана на следующем рисунке

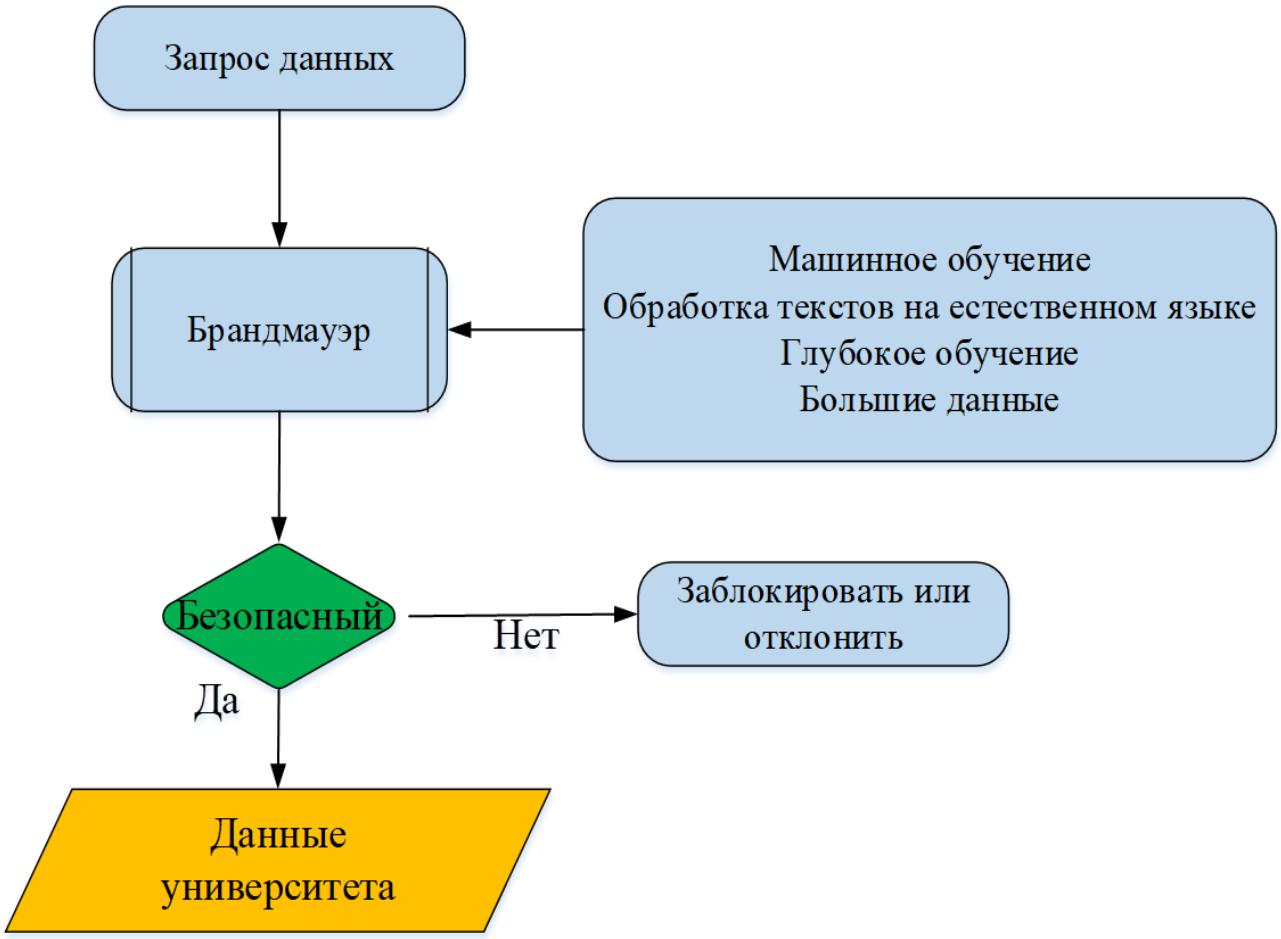

Рисунок 1 - Структура брандмауэра с использованием методов искусственного интеллекта [составлено автором]

Данный тип методов искусственного интеллекта относится к категории обучения с учителем (Supervised Learning), поскольку основан на предварительно обученной модели.

Важно отметить, что сам источник аномального запроса может использоваться в качестве признака. Таким источником может быть адрес электронной почты, номер телефона или приложение социальной сети. В случае, если источник является неизвестным или подозрительным, он может быть отнесён к категории запрещённых [6-7-8].

Другим направлением кибератак может быть взлом паролей от личных учётных записей в университетах посредством поддельных отпечатков пальцев, сканирования ладоней или распознавания лиц.

Искусственный интеллект может применять подходы для обработки биометрических сканов лица, ладони или отпечатков пальцев, такие как рекуррентные нейронные сети (Recurrent Neural Networks) [9] или визуальные трансформеры (Visual Transformers) [**Ошибка! Источник ссылки не найден.**], с целью сопоставления с сохранёнными эталонными образцами в базе данных.

На основе вычисленного коэффициента схожести ИИ способен определить, является ли попытка входа безопасной. В случае небезопасного сканирования система предложит дополнительную (вторичную) аутентификацию, например, отправку кода подтверждения на электронную почту или номер телефона. На рисунке ниже показана эта структура (Рис 3).

Все перечисленные признаки относятся к биометрическим, и они являются уникальными для каждого студента. Однако в некоторых случаях студент может использовать одно и то же изображение для получения доступа — такое изображение является офлайн-образом. В этом случае система может распознать запрос как небезопасный и запросить ввод кода аутентификации.

Основной подход в данном случае основан на методах обработки изображений, что требует выполнения операций по обработке изображений, извлечению признаков, а также построению матриц сходства между изображениями.

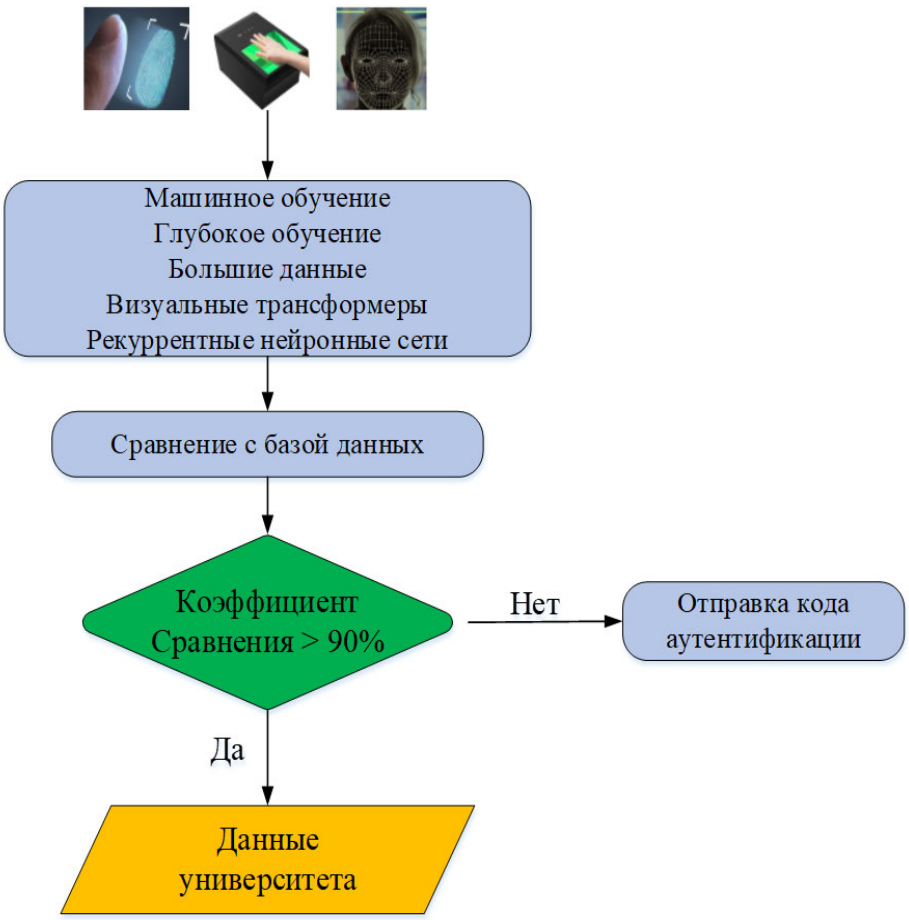

Рисунок 3 - Структура использования искусственного интеллекта с биометрическими данными [составлено автором]

Это обеспечивает поддержку входа в систему с использованием смартфонов, ноутбуков или даже устройств, применяемых при входе в университет, таких как устройства для сканирования ладони.

Таким образом, интеграция научных и этических норм, а также принципов социальной ответственности на всех этапах жизненного цикла систем ИИ — от исследований и разработки до сбора, анализа, обработки и хранения данных — может способствовать устойчивому и безопасному развитию технологий искусственного интеллекта, повышая доверие общества к данным инновациям.

Список литературы:

1. Dornseif M. et al. Teaching data security at university degree level //Proceedings of the IFIP TC11 WG. – 2005. – Т. 11. – С. 213-222.
2. Li J., Xiao W., Zhang C. Data security crisis in universities: Identification of key factors affecting data breach incidents. Humanities and Social Sciences Communications. – 2023. – No. 10 (1). – P. 270.
3. Гущина А. А., Пчелинцева Н. В., Шацкий В. А. Применение искусственного интеллекта в обеспечении безопасности данных //Инженерное обеспечение инновационных технологий в АПК. – 2021. – С. 79-81.
4. Yinka-Banjo C., Ugot O. A. A review of generative adversarial networks and its application in cybersecurity //Artificial Intelligence Review. – 2020. – Т. 53. – С. 1721-1736.
5. Prinsloo P., Slade S. Student data privacy and institutional accountability in an age of surveillance //Using data to improve higher education: Research, policy and practice. – Rotterdam: SensePublishers, 2014. – Pp. 197-214.
6. Беспалова Н. В. и др. Анализ зарубежного опыта применения интеллектуальных методов в задачах защиты объектов критической информационной инфраструктуры финансового сектора //Инженерный вестник Дона. – 2024. – №. 5 (113). – С. 8-12.
7. Яковишин А. Д. Развитие алгоритмов ИИ для обнаружения и предотвращения кибератак //Дневник науки. – 2024. – №. 1.
8. Al-Khassawneh Y. A. A review of artificial intelligence in security and privacy: Research advances, applications, opportunities, and challenges //Indonesian Journal of Science and Technology. – 2023. – Т. 8. – №. 1. – С. 79-96.
9. Huang L. Ethics of artificial intelligence in education: Student privacy and data protection //Science Insights Education Frontiers. – 2023. – Т. 16. – №. 2. – С. 2577-2587.
10. KP S. et al. RNNSecureNet: Recurrent neural networks for Cyber security use-cases //arXiv preprint arXiv:1901.04281. – 2019.

References:

1. Dornseif M. et al. Teaching data security at university degree level //Proceedings of the IFIP TC11 WG. - 2005. - Vol. 11. - P. 213-222.
2. Li J., Xiao W., Zhang C. Data security crisis in universities: Identification of key factors affecting data breach incidents. Humanities and Social Sciences Communications. - 2023. - No. 10 (1). - P. 270.

3. Gushchina A. A., Pchelintseva N. V., Shatsky V. A. Application of artificial intelligence in ensuring data security // Engineering support of innovative technologies in the agro-industrial complex. - 2021. - P. 79-81.
4. Yinka-Banjo C., Ugot O. A. A review of generative adversarial net-works and its application in cybersecurity // Artificial Intelligence Review. - 2020. - Vol. 53. - P. 1721-1736.
5. Prinsloo P., Slade S. Student data privacy and institutional accountability in an age of surveillance // Using data to improve higher education: Research, policy and practice. - Rotterdam: SensePublishers, 2014. - pp. 197-214.
6. Bespalova N. V. et al. Analysis of foreign experience in applying intelligent methods in the tasks of protecting critical information infrastructure objects of the financial sector // Engineering Bulletin of the Don. - 2024. - No. 5 (113). - P. 8-12.
7. Yakovishin A. D. Development of AI algorithms for detecting and preventing cyberattacks // Science Diary. - 2024. - No. 1.
8. Al-Khassawneh Y. A. A review of artificial intelligence in security and privacy: Research advances, applications, opportunities, and challenges // Indonesian Journal of Science and Technology. - 2023. - Vol. 8. - No. 1. - P. 79-96.
9. Huang L. Ethics of artificial intelligence in education: Student privacy and data protection // Science Insights Education Frontiers. - 2023. - Vol. 16. - No. 2. - P. 2577-2587.
10. KP S. et al. RNNSecureNet: Recurrent neural networks for Cyber security use-cases //arXiv preprint arXiv:1901.04281. – 2019.