Литература

1. Hochreiter S., Schmidhuber J. Long short-term memory //Neural computation. – 1997. – Т. 9. – №. 8. – С. 1735-1780.
2. Casado M. et al. SANE: A Protection Architecture for Enterprise Networks //USENIX Security Symposium. – 2006. – Т. 49. – С. 50.
3. McKeown N. et al. OpenFlow: enabling innovation in campus networks //ACM SIGCOMM computer communication review. – 2008. – Т. 38. – №. 2. – С. 69-74.
4. Datasets. Research. Canadian Institute of cybersecurity. https://www.unb.ca/cic/datasets/index.html (Accessed 25 March 2021).
5. Kurochkin I. I., Volkov S. S. Using GRU based deep neural network for intrusion detection in software-defined networks //IOP Conference Series: Materials Science and Engineering. – IOP Publishing, 2020. – Т. 927. – №. 1. – С. 012035.
6. Volkov S. S., Kurochkin I. I. Network attacks classification using Long Short-term memory based neural networks in Software-Defined Networks //Procedia Computer Science. – 2020. – Т. 178. – С. 394-403.
7. Carlson L., Okurowski M. E., Marcu D. RST discourse treebank. – Linguistic Data Consortium, University of Pennsylvania, 2002.
8. Wang Y., Li S., Wang H. A two-stage parsing method for text-level discourse analysis //Proceedings of the 55th Annual Meeting of the Association for Computational Linguistics (Volume 2: Short Papers). – 2017. – С. 184-188.
9. Devlin J. et al. Bert: Pre-training of deep bidirectional transformers for language understanding //arXiv preprint arXiv:1810.04805. – 2018.

Р.М. Ганеев, А.А. Столбова

ПРОЕКТИРОВАНИЕ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ ВЫЯВЛЕНИЯ ПОДДЕЛЬНЫХ АККАУНТОВ В СОЦИАЛЬНЫХ СЕТЯХ

(Самарский университет)

Использование поддельных аккаунтов является одним из наиболее распространенных способов для совершения злонамеренных действий в социальных сетях: рассылка спама, мошенничество или иное злоупотребление возможностями социальной сети. Своевременное обнаружение и принятие мер в отношении таких аккаунтов необходимы для защиты подлинных участников социальных сетей, а также для поддержания надежности самой сети. Тем не менее, любой поддельный аккаунт может иметь правдоподобный и заполненный профиль что делает его неотличимым от подлинных аккаунтов и существенно затрудняет обнаружение [1, 2].

В рамках данной работы предлагается разработать автоматизированную систему, позволяющую выявлять поддельные аккаунты в социальных сетях. В качестве исследуемой социальной сети выбрана сеть «ВКонтакте», поскольку данная сеть занимает лидирующую позицию в рейтинге социальных сетей по

количеству посещений в месяц среди пользователей на территории России, согласно данным Mediascope WEB-Index [3].

Общий рейтинг операционных систем, включая настольные компьютеры, ноутбуки и смартфоны, показывает, что лидером является операционная система Android, которая установлена более чем на 39% устройствах [4], поэтому данная операционная система выбрана в качестве целевой.

К функциональным возможностям системы относятся:

– возможность анализа страницы пользователя социальной сети;
– возможность просмотра истории проверок;
– пользовательская настройка автоматизированной системы.

Возможность анализа страницы пользователя социальной сети заключается в определении подлинности данной страницы. Определим критерии, по которым система должна определять подлинность страницы:

– статус страницы (удалена, заблокирована);
– наличие верификации;
– дата регистрации;
– дата последнего посещения страницы;
– дата последнего изменения страницы;
– количество исходящих подписок;
– количество подписчиков;
– количество друзей;
– количество фейковых, удаленных, заблокированных друзей;
– количество групп;
– количество записей на стене;
– даты публикаций записей;
– количество фото;
– дата загрузки фото;
– оригинальность аватарки.

Функция просмотра истории результатов предоставляет доступ пользователю к удалению и открытию определённого результата анализа.

Пользовательская настройка автоматизированной системы позволяет пользователю настроить систему индивидуально, а именно установить «ночную» тему или режим левши.

Для проектирования автоматизированной системы применялся язык UML, одновременно являющийся простым и мощным средством моделирования, который может быть эффективно использован для построения концептуальных, логических и графических моделей сложных систем различного целевого назначения [5]. На рисунке 1 представлена разработанная диаграмма вариантов использования автоматизированной системы выявления поддельных аккаунтов в социальных сетях.

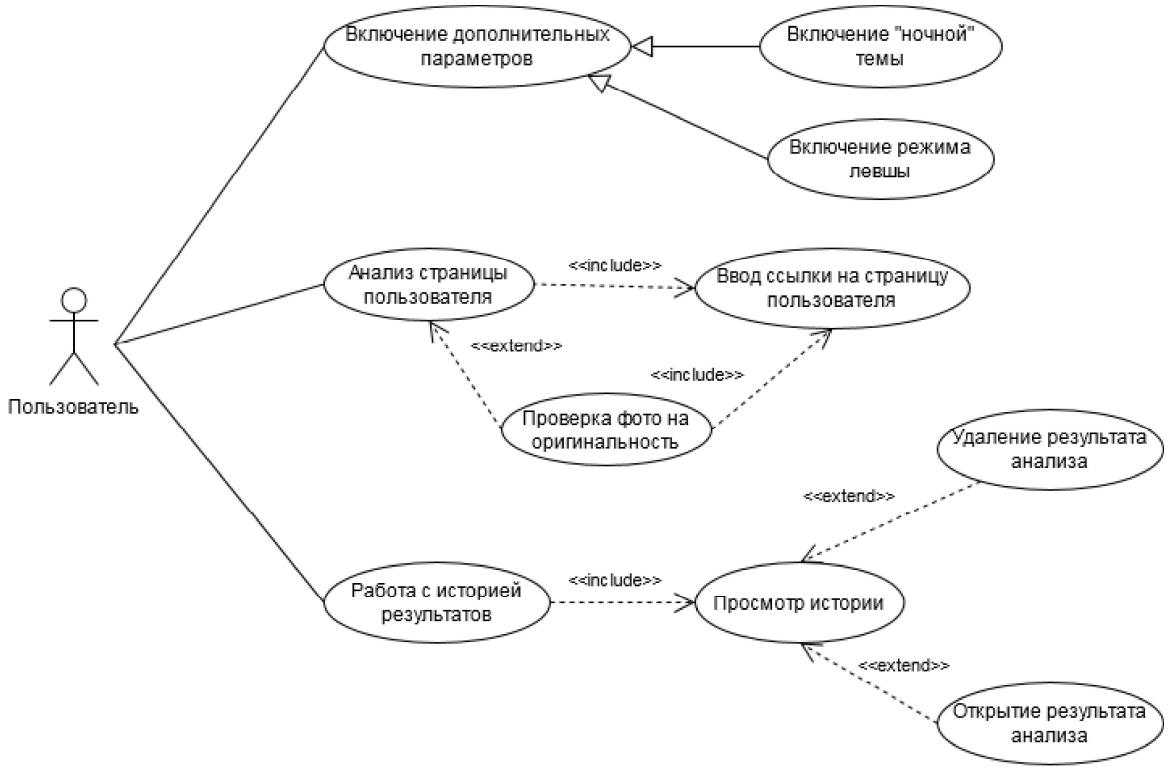

Рисунок 1 – Диаграмма вариантов использования автоматизированной системы выявления поддельных аккаунтов в социальных сетях

Разрабатываемая автоматизированная система состоит из следующих модулей:

1) *Модуль генерации запроса* необходим для правильного конструирования запроса к «ВКонтакте API» и foaf.php.

2) *Модуль сбора данных* состоит из «ВКонтакте API», который необходим для получения основной информации, foaf.php, предоставляющего даты регистрации, последнего входа и последнего изменения страницы, а также модуля обработки фото. Модуль обработки фото получает ссылку на главную фотографию пользователя от «ВКонтакте API» и далее оригинальность фото определяется с помощью «API Поиск по Яндекс.картинкам».

3) *Модуль анализа данных* представляет из себя обученную нейронную сеть, которая классифицирует полученную информацию и выдает конечный результат проверки аккаунта на подлинность

4) *Модуль обработки информации* получает данные от предыдущих модулей и заполняет профиль проверенного аккаунта для его дальнейшего сохранения в базу данных.

5) *Модуль взаимодействия с базой данных* обеспечивает работу с базой данных, в которой хранятся данные о профилях.

Структурная схема разрабатываемой автоматизированной системы представлена на рисунке 2.

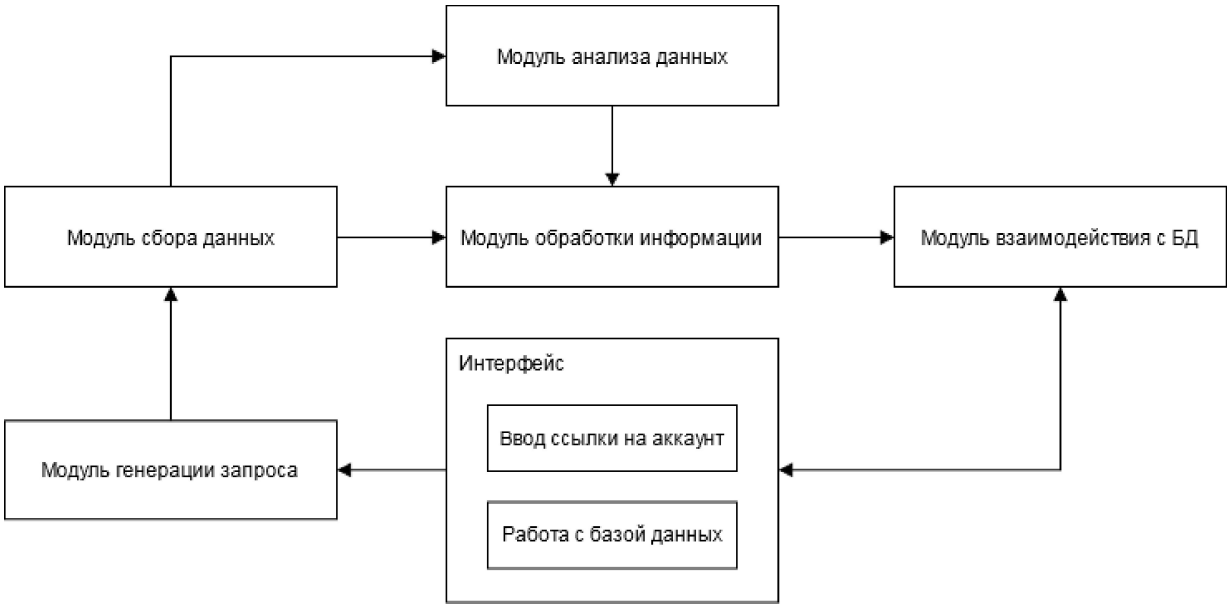

Рисунок 2 – Структурная схема автоматизированной системы выявления поддельных аккаунтов в социальных сетях

Таким образом, в результате данной работы спроектирована автоматизированная система выявления поддельных аккаунтов в социальных сетях, определены основные функциональные возможности системы, выявлены критерии определения подлинности аккаунта, разработана структурная схема системы.

Литература

1. Ivaschenko A. et al. Modeling of user behavior for social media analysis //2018 Moscow Workshop on Electronic and Networking Technologies (MWENT). – IEEE, 2018. – С. 1-4.

2. Xiao C., Freeman D. M., Hwa T. Detecting clusters of fake accounts in online social networks // Proceedings of the 8th ACM Workshop on Artificial Intelligence and Security. – 2015. – С. 91-101.

3. Аудитория интернета в России [Электронный ресурс]. – https://webindex.mediascope.net/ (дата доступа 16.04.2021).

4. Статистика [Электронный ресурс]. – https://statcounter.com/ (дата доступа 16.04.2021).

5. Пайлон Д. UML 2 для программистов / Д. Пайлон – М.: Питер. – 2012. – С. 198.