ISSN 2949-2726

Hi-Hume Journal

ЖУРНАЛ ВЫСОКИХ ГУМАНИТАРНЫХ ТЕХНОЛОГИЙ

№1 (1) 2023

ISSN 2949-2726 Hi-Hume Journal — Журнал высоких гуманитарных технологий 2023 №1(1) Апрель — июнь

ISSN 2949-2726

Hi-Hume Journal **№ 1 (1)**

Журнал высоких гуманитарных технологий **2023**

Ежеквартальное научное издание **Апрель—июнь**

Свидетельство государственной регистрации:
Эл № ФС 77-83536 от 13.07.2022

Выходит 4 раза в год (ежеквартально).

Возрастная категория: 16 +

В журнале публикуются статьи по научным специальностям:

2.3. Информационные технологии и телекоммуникации

5.9. Филология

5.10. Искусствоведение и культурология

Издание для научных работников, преподавателей высшей школы, аспирантов, студентов и всех, кто интересуется достижениями современной российской науки.

Вёрстка: Шухер П.Д.
Корректор: Бальтерманц Л. Ф.

Учредитель: Былевский П. Г.

Издатель: Институт информационных наук Московского государственного лингвистического университета

Адрес редакции:
119034 Россия, Москва, ул. Остоженка, 36

https://www.linguanet.ru

E-mail: hi-hume@yandex.ru

Номер подписан в печать 10.06.2023

СОДЕРЖАНИЕ

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ

ФИЛОЛОГИЯ

ИСКУССТВОВЕДЕНИЕ И КУЛЬТУРОЛОГИЯ

CONTENT

INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

PHILOLOGY

ART HISTORY AND CULTURAL STUDIES

УДК 004.056

МОДЕРНИЗАЦИЯ МЕТОДОЛОГИИ: СТРАТЕГИЯ И ТАКТИКА ПРОТИВОДЕЙСТВИЯ «ТЕЛЕФОННЫМ МОШЕННИЧЕСТВАМ»

Былевский П. Г.
Московский государственный лингвистический университет
(Россия, Москва)
e-mail: pr-911@yandex.ru

Гатауллин С. Т.
Московский технический университет связи и информатики (Россия, Москва)
e-mail: s.t.gataullin@mtuci.ru

Плешакова Е. С.
Финансовый университет при Правительстве РФ (Россия, Москва)
e-mail: espleshakova@fa.ru.

Аннотация

В статье проанализированы новейшие тенденции и вопросы модернизации методологии противодействия телефонному мошенничеству. Представлена улучшенная классификация задач на тактические (выявление и блокировка) и стратегические (предупреждение и профилактика), их реализация в методологии и нормативной деятельности. Исследованы актуальные меры развития методологической и нормативной деятельности, законодательства в сочетании с организационными, техническими и другими методами финансовых организаций, участников отраслевой телекоммуникационной инфраструктуры и правоохранительных органов. Определены средства повышения эффективности взаимодействия в противодействии телефонным и другим мошенничествам в телекоммуникационной инфраструктуре банков и государственных структур. Результаты подтверждаются эффективностью применения предлагаемых принципов, сделаны выводы о необходимости оперативного совершенствования методологии соответственно новейшим тенденциям развития телефонных и других мошенничеств.

Ключевые слова
Информационная безопасность, телефонные мошенничества, дистанционные финансовые сервисы, противодействие, методология, нормативно-правовая база

Статья подготовлена в рамках государственного задания Правительства Российской Федерации Финансовому университету на 2022 год по теме «Модели и методы защиты текстов в рамках противодействия телефонному мошенничеству» (ВТК-ГЗ-ПИ-30–2022).

Для цитирования: Былевский П. Г., Гатауллин С. Т., Плешакова Е. С. Модернизация методологии: стратегия и тактике противодействие «телефонным мошенничествам» // Hi-Hume Journal.—2023.—№ 1 (1).—С. 6–16.

MODERNIZATION OF METHODOLOGY: STRATEGY AND TACTICS OF COUNTERING "TELEPHONE FRAUD"

Pavel G. Bylevskiy
Moscow State Linguistic University (Moscow, Russia)
e-mail: pr-911@yandex.ru

Sergei T. Gataullin
Moscow Technical University of Communications and Informatics (Moscow, Russia)
e-mail: s.t.gataullin@mtuci.ru

Ekaterina S. Pleshakova
Financial University under the Government of the Russian Federation (Moscow, Russia)
e-mail: espleshakova@fa.ru.

Abstract
The article analyzes the latest trends and issues of modernization of the methodology of countering telephone fraud. The improved classification of tasks into tactical (detection and blocking) and strategic (prevention and prevention), their implementation in methodology and regulatory activities is presented. The current measures for the development of methodological and regulatory activities, legislation in combination with organizational, technical and other methods of financial organizations, participants in the industry

telecommunications infrastructure and law enforcement agencies are studied. The means of increasing the effectiveness of interaction in countering telephone and other frauds in the telecommunications infrastructure of banks and government agencies have been identified. The results are confirmed by the effectiveness of the application of the proposed principles, conclusions are drawn about the need for operational improvement of the methodology according to the latest trends in the development of telephone and other frauds.

Keywords
Information security, telephone fraud, remote financial services, counteraction, methodology, regulatory framework

The article was prepared as part of the state assignment of the Government of the Russian Federation to the Financial University for 2022 on the topic «Models and methods of text protection in the framework of countering telephone fraud» (VTK-GZ-PI-30–2022).

For citation: Bylevskiy P. G., Gataullin S. T., Pleshakova E. S. Modernization of methodology: strategy and tactics of countering "telephone fraud" // Hi-Hume Journal.—2023.—№ 1 (1).—Pp. 6–16.

Введение

Телефонные мошенничества, в частности, очень распространены и наносят значительный ущерб, но всё же это достаточно специализированный вид нарушений информационной безопасности [1]. Следует учитывать, что методология противодействия телефонным мошенничествам и другим подобным нарушениям в телекоммуникационной инфраструктуре банков и государственных структур разрабатывается и реализуется в тесной связи с организационными, техническими и другими аспектами, включая методологию, нормативные инструменты и развитие законодательства. Против телефонного мошенничества нет отдельных законодательных актов, но есть те, что имеют более или менее прямое, а также важное косвенное отношение.

Среди инструментов противодействия подобным нарушениям и преступлениям предлагается методологически определить «смысловое ядро» и его «периферию». Во-первых, в нормативном, в том числе законодательном, обеспечении противодействия преступлениям в финансовой сфере, совершаемых с использованием компьютерно-телекоммуникационных средств, следует выделять, с одной стороны,

непосредственно, а с другой стороны, опосредованно относящиеся к телефонным мошенничествам. Во-вторых, подразделять организационно-технические меры и инструменты на два направления: тактическое предупреждение (оперативное реагирование) и стратегическое противодействие этому виду преступлений.

Соотношение реагирования и предупреждения инцидентов

Увеличение количества и разнообразия телефонных мошенничеств в последние годы сопровождалось совершенствованием методологии противодействия, включая развитие законодательства, связанного с применением организационно-технических инструментов противодействия таким нарушениям [2]. Можно классифицировать направления деятельности государственных органов, финансовых и других организаций, направленных на противодействие телефонным мошенничествам, включая профилактику и предупреждение [3]. Оперативное реагирование (выявление и пресечение) и предупреждение, профилактика — два различных, но взаимосвязанных направления противодействия телефонным мошенничествам.

Телефонные мошенничества принадлежат к нарушениям и преступлениям, наносящим гражданам и организациям имущественный ущерб преимущественно в денежной форме [4]. Они связаны с компьютерными инцидентами, в особенности в финансовой сфере, но не сводятся к ним. У телефонных мошенничеств есть своя узкая специфика, но в то же время и одинаковые черты с другими видами правонарушений с использованием компьютерных и телекоммуникационных средств [5]. Особенность телефонных мошенничеств в том, что главным инструментом является «социальная инженерия» — психологические приёмы обмана, вхождения в доверия. Компьютерные и телекоммуникационные технологии выступают второстепенными, техническими инструментами действий, которые совершает обманутая мошенниками жертва [6].

Предупреждение и профилактика являются важным направлением правоохранительной политики в противодействии таким правонарушений и преступлениям, элементом обеспечения информационной безопасности финансовых сервисов [7]. Предупреждение — задача тактического характера, заключается в предотвращении телефонных мошенничеств посредством правильного оперативного реагирования, благодаря своевременному выявлению и пресечению подобных попыток хищений [8]. Суть профилактики стратегическая, в определении и устранении уязвимостей защиты дистанционных финансовых серви-

сов и других предпосылок, способствующих подготовке и совершению телефонных мошенничеств [9].

Методология квалификации преступлений и тяжести ответственности

Соответствие строгости наказания размерам нанесённого ущерба и общественной опасности является важным сдерживающим фактором для злоумышленников [10]. Российская юриспруденция вслед за зарубежным опытом движется в направлении всё большей детализации уголовного законодательства в отношении преступлений, совершаемых при помощи компьютерно-телекоммуникационных технических средств [11]. Инерция квалификации таких криминальных действий как «неправомерного доступа к информации» давно не отвечала многообразию, многочисленности, размерам наносимого ущерба и степени общественной опасности. Вплоть до 2012 года в Уголовном Кодексе РФ был только один, обобщённый состав мошенничества. Хищения в дистанционном банковском обслуживании определялись как мошенничества расширенно, даже когда совершались без ведома законных владельцев средств, при помощи тайно похищенных данных для управления их банковскими счетами.

Федеральный закон от 29 ноября 2012 года № 207-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» открывал перспективу квалифицировать в ст. 1596 подобные преступления не как мошенничество, а как кражу. Было проведено разграничение с компьютерными преступлениями, связанными с несанкционированным доступом к информации, преодолением средств защиты с нелегальным использованием программно-аппаратными средств, но без обмана или злоупотребления доверием.

Появились специальные статьи Уголовного Кодекса РФ, квалифицирующие разные типы мошеннических действий в различных областях: при выдаче кредитов, в страховых услугах и применительно к другим видам финансовых услуг, оказываемых с использованием компьютерно-телекоммуникационных технологий.

Отделение других видов преступлений использованием компьютерно-телекоммуникационных технологий позволило ужесточить ответственность соразмерно размерам наносимого ущерба и общественной опасности за собственно мошенничество, включая телефонное—завладение чужими денежными средствами путём обмана, преднамеренного введения в заблуждение [12]. Срок лишения свободы

за такое преступления стало возможным увеличить согласно ст. 1596 Уголовного Кодекса РФ до 5 лет.

Дальнейшая конкретизация и детализация подобных правонарушений и преступлений развивается с учётом часто встречающихся случаев наличия во многих преступлениях смешанных признаков различных специализированных составов [13]. Юристы понимают, что всё большая детализация многообразия преступлений в дистанционных финансовых сервисах с использованием компьютерно-телекоммуникационных средств не должна чрезмерно усложнять практику применения правовых норм [14].

Ужесточается ответственность за их разработку, подготовку и осуществление телефонных мошенничеств: в 2011 году были изменены ст. 272, 273 и 274 гл. 28 Уголовного Кодекса РФ. Была усилена уголовная ответственность и за другие преступления в области электронных финансовых услуг. Квалификация подобных преступлений как краж, тайного хищения чужого имущества, прежде соответствовала ч. 1 ст. 158 Уголовного Кодекса, предусматривая в качестве ответственности лишение свободы на срок до двух лет. Изменения, внесённые в федеральное законодательство, сделали возможным подпадание таких правонарушений под действие ч. 3 ст. 158-й не как небольшой степени тяжести, а как тяжких преступлений. Срок лишения свободы за них по новой квалификации возрастает до шести лет.

Правовые новации повышают ответственность также за мошенничества, совершаемые с применением различных компьютерно-телекоммуникационных устройств и финансовых сервисов: интернет-банкинга, банковских карт, мобильных платёжных приложений, электронных торговых площадок, и, в этом контексте, мобильных телефонов как средства голосовой связи и доступа в интернет [15]. Были сняты ограничения состава преступлений операциями с банковскими картами с наказанием в виде штрафа, без лишения свободы. Расширение и уточнение квалификации таких преступлений позволяет увеличить ответственность вплоть до лишения свободы сроком до 3 лет.

Модернизация организационно-технического и нормативного противодействия телефонным мошенничествам

Деятельность по противодействию, предупреждению и профилактике, защиты граждан от телефонных мошенничеств нуждаются в нормативном, в первую очередь законодательном обеспечении [16]. Основные направления модернизации этой деятельности и развития законодательства в последние годы таковы:

— усиление неотвратимости ответственности за телефонные мошенничества (облегчение расследований, оперативно-розыскной и следственной деятельности, уголовно-процессуальных действий и судебных разбирательств);

— ужесточение наказаний до соразмерности характеру общественной опасности и наносимому ущербу путём уточнения юридической квалификация и повышения строгости наказания;

— снижение количества эксплуатируемых телефонными мошенниками организационно-технических уязвимостей в оборудовании, программном обеспечении, компьютерно-телекоммуникационных системах и архитектурах информационной безопасности;

— совершенствование мер выявления и блокировки организационно-технических возможностей использования преступниками похищенных денежных средств, соотносимое с противодействием отмыванию доходов;

— выстраивание единой системы мониторинга и анализа для выявления и оперативного реагирования на попытки телефонного мошенничества;

— создание доступной ключевым субъектам противодействия централизованной структурированной базы оперативно обновляемых данных о телефонных мошенничествах, включая описания инцидентов, персональные данные и реквизиты участников подозрительных транзакций, номера мобильных телефонов и т.п.;

— развитие регламентов и механизмов дополнительной идентификации участников транзакций, мотивированного отказа в обслуживании и блокировки подозрительных или оспариваемых действий, возвращения денежных средств легальным владельцам;

— сокращение возможностей анонимного и нелегального использования SIM-карт, подменных телефонных номеров, а также доступа в интернет [17].

Законодательные нововведения и другие нормативные инструменты необходимы для обеспечения «тактических» мер предупреждения—своевременного выявления и блокировке попыток телефонного мошенничества [18].

К таким мерам относится создание централизованных защищённых баз данных, доступных участникам системы защиты от телефонных мошенничеств —государственных организаций (отраслевые регулирующие и правоохранительные органы), коммерческих компаний (в первую очередь оказывающих финансовые услуги), а также гражданам и организациям—клиентам финансовых услуг [19].

Изменения методологии противодействия, введение ряда новых правовых норм также нужны для оперативного пополнения доступных «чёрных списков» признаков мошенничества — подозрительных телефонных номеров [20], организаций и граждан, интернет-ресурсов [21]. Такие сервисы определения нежелательных и подозрительных номеров входящих телефонных звонков уже широко создаются и работают при участии граждан, на основе анализа их отзывов («Не бери трубку», в «Яндексе» и др.). Нужна доработка подобных решений, повышение эффективности, защищённости, интеграции и централизации до индустриальных параметров на федеральном уровне [21]. Развитие методологии, нормативных документов, законодательства направлено и на обеспечение «стратегических» профилактических мер. Такие меры нацелены на ликвидацию преимуществ трансграничности для злоумышленников, возможностей совершать мошенничества, находясь за рубежом или используя расположенные за границей сообщников, технические средства [22].

Выводы

Проведенный анализ показывает актуальность конкретизации методологии противодействия в виде разделения методологического и нормативного инструментария на задачи тактического реагирования, предупреждения и стратегической профилактики телефонных мошенничеств. К тактическому направлению относятся «ручное» и автоматизированное выявление попыток совершения подобных нарушений [23], блокировка развития таких инцидентов, устранение последствий, расследование и возмещение ущерба. К стратегическому следует относить устранение условий, предпосылок для правонарушений и преступлений, относящихся к телефонным мошенничествам. Предлагаемое структурирование способно повысить эффективность методологии противодействия, продуктивность взаимодействия специалистов по информационной безопасности финансовой сферы, правоохранительных органов и законодателей в противодействии телефонным мошенничествам.

Список источников

1. Кулев В. К., Папшева Е. В., Старинский А. Ю., Сугробова К. С. Телефонное мошенничество // Труды международного симпозиума «Надежность и качество». Пензенский государственный университет. –Т. 2. –2010. — С. 352–354.

2. Веселов Ю. В. Доверие и обман в цифровом мире // Международный форум Kazan Digital Week—2021. Сборник материалов.—Казань, ГБУ «НЦБЖД»: 2021.—С. 269–274.

3. Рясова А. И. К вопросу профилактики мошенничеств с использованием средств мобильной связи и компьютерных технологий лицами, отбывающими наказание в виде лишения свободы / Информационные технологии как основа прогрессивных научных исследований. Сборник статей Международной научно-практической конференции.—Уфа: ООО «Аэтерна», 2022.—С. 111–116.

4. Vasiliev N., Pavlov N., Osipov A., Ivanov M., Pleshakova E., Korchagin S., Victor R., Konstantin B. Development of the intelligent object detection system on the road for self-driving cars in low visibility conditions // Studies in Computational Intelligence.—2022.—Т. 1032 SCI.—С. 576–584.

5. Zhang A., Bradford B., Morgan R. M., Nakhaeizadeh C. Investigating the uses of mobile phone evidence in China criminal proceedings // Science & Justice.—2022.—Vol. 62.—№ 3.—P. 385–398.

6. Гилязов Р. Р. Способы совершения телефонных мошенничеств как элемент криминалистической характеристики // Актуальные проблемы государства и общества в области обеспечения прав и свобод человека и гражданина.—2015.—№ 18–3.—С. 259–262.

7. Васильченко Д. А., Десятов М. С. Оперативно-розыскная характеристика способов совершения «телефонных мошенничеств» // Актуальные вопросы организации и правового регулирования деятельности оперативных подразделений МВД России (посвящается памяти профессора Д. В. Ривмана). Материалы региональной научно-практической конференции.—Санкт-Петербургский университет Министерства внутренних дел Российской Федерации (Санкт-Петербург): 2016.—С. 135–138.

8. Liu D., Lee J-H. CFLedger: Preventing chargeback fraud with blockchain // ICT Express. —2022.—Vol. 8.—№ 3.—P. 352–356.

9. Ivanov M., Radygin V., Korchagin S., Pleshakova E., Sheludyakov D., Yerbayev Y., Bublikov K. Intelligent web-application for countering ddos attacks on educational institutions // Studies in Computational Intelligence. 2022.—Т. 1032 SCI.—С. 182–194.

10. Ущекин С. Н. Хищение денежных средств с использованием информационных технологий. Проблемы раскрытия и расследования органами внутренних дел // Евразийский юридический журнал.—2022.—№ 3 (166).—С. 343–345.

11. Yelland M. Fraud in mobile networks // Computer Fraud & Security.—2013.—2013.—№ 3.—P. 5–9.

12. Chen S., Yuan Y., Luo X., Wang Y. Discovering group-based transnational cyber fraud actives: A polymethodological view // Computers & Security. — 2021. — Vol. 104. https://doi.org/10.1016/j.cose.2021.102217

13. Bruns R., Dunkel J., Offel N. Learning of complex event processing rules with genetic programming // Expert Systems with Applications. — 2019. — Vol. 129. — P. 186–199. https://doi.org/10.1016/j.eswa.2019.04.007.

14. Ribaux O., Souvignet T. "Hello are you available?" Dealing with online frauds and the role of forensic science // Forensic Science International: Digital Investigation. — 2020. — Vol. 33. 300978. https://doi.org/10.1016/j.fsidi.2020.300978.

15. Воронина И. А. Применение технологии блокчейн в России и за рубежом: проблема правового регулирования / Устойчивое развитие, открытое мышление и цифровые трансформации. Сборник материалов Всероссийской конференции с международным участием. — Астрахань, ИП Сорокин Роман Васильевич: 2022. — С. 149–167.

16. Леонов М. В. Методологические аспекты организации обращения национальной цифровой валюты / Russian economic bulletin. –2021. — Т. 4. — № 6. — С. 150–156.

17. Семенова Н. А. Запрет анонимности в сети интернет как мера профилактики мошенничества // Современная наука: актуальные проблемы теории и практики. Серия: экономика и право. — 2022. — № 3. — С. 177–182.

18. Kempa M. S., Peng Y. Machine learning algorithms for fraud prediction in property insurance: Empirical evidence using real-world microdata // Machine Learning with Applications. — 2021. — Vol. 5. — P. 1–14. https://doi.org/10.1016/j.mlwa.2021.100074.

19. Коротеев М. В., Плешакова Е. С., Желябин Д. В. Обзор методов nlp, используемых для распознавания текста с целью противодействия телефонному мошенничеству // Безопасность бизнеса. — 2022. — С. 46–51.

20. Германович А. В., Мельников С. Ю., Пересыпкин В. А., Сидоров Е. С., Цопкало Н. Н. Информационные измерения языка. Программная система оценки читаемости искаженных текстов // Известия ЮФУ. Технические науки. — 2019. — № 7 (209). — С. 6–17.

21. Барабанов В. С. К вопросу о телефонном мошенничестве // Научно-практический электронный журнал Аллея науки. — 2018. — Т. 2. — № 6 (22). — С. 785–790.

22. Литвинов Н. Д., Федоров А. Н. Мошенничество с использованием средств мобильной связи (дистанционное): понятие и особенности совершения // Научно-исследовательские публикации. Общество

с ограниченной ответственностью «Вэлборн» (Воронеж).—2015.—№ 12 (32).—С. 73–80.

23. Zhang J., Tian C., Zhenhua Z. An efficient approach for taint analysis of android applications // Computers & Security.—2021.—Vol. 104. https://doi.org/10.1016/j.cose.2020.10216.

Об авторах

Былевский Павел Геннадитвич—
кандидат философских наук, доцент;
Московский государственный
лингвистический университет
(Россия, Москва).
E-mail: pr-911@yandex.ru.

Гатауллин Сергей Тимурович—
кандидат экономических наук, декан
факультета «Цифровая экономика
и массовые коммуникации» Московского
технического университета связи
и информатики (Россия, Москва),
ведущий научный сотрудник
Департамента информационной
безопасности факультета
информационных технологий и анализа
больших данных Финансового
университета при Правительстве РФ
(Россия, Москва).
E-mail: s.t.gataullin@mtuci.ru.

Плешакова Екатерина Сергеевна—
кандидат технических наук, доцент
Департамента информационной
безопасности факультета
информационных технологий и анализа
больших данных Финансового
университета при Правительстве РФ
(Россия, Москва).
E-mail: espleshakova@fa.ru.

About the authors

Pavel G. Bylevskiy —
Candidate of Philosophical Sciences,
Associate Professor; Moscow State
Linguistic University
(Russia, Moscow).
E-mail: pr-911@yandex.ru.

Sergey T. Gataullin—
PhD in Economics, Dean of the
Faculty of Digital Economy and
Mass Communications of the
Moscow Technical University of
Communications and Informatics
(Moscow, Russia), leading researcher
at the Department of Information
Security of the Faculty of Information
Technology and Big Data Analysis of
the Financial University under the
Government of the Russian Federation
(Moscow, Russia).
E-mail: s.t.gataullin@mtuci.ru.

Ekaterina S. Pleshakova —
Candidate of Technical Sciences,
Associate Professor of the Department
of Information Security of the Faculty
of Information Technology and Big Data
Analysis of the Financial University
under the Government of the Russian
Federation (Russia, Moscow).
E-mail: espleshakova@fa.ru.

УДК 51-7, 004.056

SOC КАК ИНСТРУМЕНТ ПОВЫШЕНИЯ УРОВНЯ КИБЕРБЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

Карелова О. Л.
Московский государственный лингвистический университет (Россия, Москва),
Российская академия народного хозяйства и государственной службы
при Президенте РФ (Россия, Москва),
okarelova@yandex.ru

Дробышев Е. С.
Московский государственный лингвистический университет (Россия, Москва)
2002temych2002@gmail.com

Аннотация
В статье проводится анализ работы Ситуационного центра информационной безопасности, его актуальные проблемы и процесс трансформации в нынешних мировых условиях. Рассмотрены варианты модернизации Ситуационного центра в его классической модели и методы совершенствования в модель нового поколения.

Ключевые слова
Киберугрозы, информационная безопасность, кибербезопасность, Ситуационный центр информационной безопасности (SOC).

Для цитирования: Карелова О. Л., Дробышев А. В. SOC как инструмент повышения уровня кибербезопасности организации // Hi-Hume Journal.—2023.—№ 1 (1).—С. 17—23.

SOC AS A TOOL TO INCREASE THE LEVEL OF CYBERSECURITY OF AN ORGANIZATION

Oxana L. Karelova
Moscow State Linguistic University (Russia, Moscow),
The Russian Presidential Academy of National Economy and Public Administration
(Russia, Moscow)

Artem V. Drobyshev
Moscow State Linguistic University (Russia, Moscow)
2002temych2002@gmail.com

Abstract

The article analyzes the Situational Information Security Center work, its current issues and the process of transformation under the current world conditions. Variants of the Situational Center in its classical model modernization are offered. The methods of a new generation model refinement are considered as well.

Keywords

The Situational Information Security Center (SOC), cyber threats, cybersecurity, information security.

For citation: Karelova O. L., Drobyshev A. V. SOC as a tool for increasing the level of cybersecurity of an organization // Hi-Home Journal.—2023.—№ 1 (1).—Pp. 17—23.

В современной экономической формации наиболее ценными активами являются знания и информация. Возрастающая цифровизация всех сфер жизни общества ведет к тому, что подавляющее количество информации находится в цифровом виде и эта информация является главной целью киберпреступников. Методы и средства взлома систем защиты информационной безопасности компаний все время совершенствуются. В самих компаниях, как правило, увеличивается количество точек доступа, которые потенциально могут быть использованы для проникновения в систему информации компании. Реактивное реагирование на инциденты информационной безопасности уже не обеспечивает должный уровень безопасности и защищенности информационных ресурсов.

Одним из наиболее эффективных инструментов защиты ИТ-инфраструктуры компании является Ситуационный центр информационной безопасности (Security Operation Center, далее—SOC).

SOC—это структура, объединяющая людей, процессы и технологии для достижении глобальной цели: снижения рисков через повышение киберзащиты в организации [1].

Функционал и тип (внешний, внутренний, гибридный) такого центра зависят от нужд организации.

Подавляющее большинство компаний используют SOC базового уровня. Такой Центр состоит из: SIEM-системы, занимающейся мониторингом и анализом данных, а также управлением событиями кибер-

безопасности; системы, отвечающей за сбор и анализ данных с конечных устройств; системы, которая отвечает за автоматизацию процессов и реагирование на события кибербезопасности. Эти системы выполняют рутинные задачи по сбору, анализу, реагированию и формированию отчетности о событиях кибербезопасности.

Основная аналитическая работа выполняется сотрудниками SOC, которые, как правило, делятся на две (в крупных организациях на три) линии.

Специалисты 1-й линии занимаются оперативным разбором входящей информации о событиях кибербезопасности. Если событие является инцидентом, то определяется его уровень критичности. Реагированием на инциденты низкого уровня занимаются сотрудники первой линии, а если инцидент оказывается среднего или высокого уровня критичности, то он передается специалистам второй линии SOC. Сотрудники второй линии должны обладать более глубокими экспертными компетенциями: они могут расследовать инцидент от нескольких минут до недель, собирая детальные данные, привлекая экспертов, восстанавливая последовательность действий и т.д. Помимо сотрудников первой и второй линий в команде могут быть эксперты по цифровой криминалистике и аналитики вредоносного ПО, специалисты по анализу угроз, специалисты по разработке контента для SIEM и руководитель, который отвечает за координацию SOC и смежных подразделений [2].

Такой SOC решает только задачи начального уровня по обеспечению информационной безопасности: сбор и хранение событий ИБ в едином централизованном хранилище; верхнеуровневая простая корреляция событий между различными источниками; базовая визуализация и отчетность. И имеет ряд существенных проблем. Основными проблемами являются следующие:

—большое количество ложных срабатываний SIEM. Т.е. проблема выявления действительных инцидентов в потоке событий кибербезопасности;

—использование в SIEM неэффективных правил корреляции, которые не позволяют выявлять многие актуальные угрозы ИБ;

—разрозненность и несистематизированность существующих правил корреляции SIEM, что ведет к затруднению их настройки, управления и модернизации.

—рассогласованность различных средств защиты информации, которые используются организациями, ведет к возрастанию времени на выявление инцидента кибербезопасности и, соответственно, реагирования на него;

—все большее число атак на компании носят автоматизированный характер и команда SOC не в состоянии обрабатывать такое количество событий информационной безопасности;

—попытки решить проблему повышения уровня защиты за счет увеличения штата сотрудников SOC не приносят желаемого результата. Увеличение штата замедляется скорость взаимодействия и реагирования на угрозы. Кроме того, высококвалифицированные специалисты в области кибербезопасности очень дорого стоят и дефицитны;

—нехватка достаточного количества квалифицированного персонала для выявления новых видов атак;

—отсутствие механизма автоматического определения связанности выявленных инцидентов на основе различных критериев и обнаружения целенаправленных атак [3].

Атаки киберпреступников становятся все более изощренными и целенаправленными. Обнаружение таких атак и реагирование на них требует не только достаточного объема обрабатываемых событий ИБ, но и эффективного и управляемого инструмента для выявления таких угроз.

В новых реалиях, с начала 2022 года многократно возросло количество кибератак на российские организации. По данным Solar JSOC [4] во втором квартале 2022 года количество инцидентов кибербезопасности высокого уровня критичности возросло почти в три раза. Особенность сложившейся ситуации определяют следующие факторы: большое количество (автоматизация) атак; усложнение способов и методов точечных атак на конкретные организации; эксплуатация уязвимостей в ПО, которые не устраняются в связи с невозможностью обновления из-за ухода иностранных компаний с отечественного рынка; при меньшем количестве инцидентов хватало времени на их локализацию, сейчас же ключевым фактором становится оперативность, учитывая нагрузку на операторов мониторинга, аналитиков, и других специалистов.

Еще одна крайне важная проблема, которая возникла, опять же в связи с уходом иностранных компаний—это проблема импортозамещения программных продуктов, которые используются в SOC [4]. Очевидно, что все вышеперечисленные проблемы требуют решения в рамках SOC.

Определенно, работа специалистов SOC стала значительно напряженнее. В разы возросло количество инцидентов среднего и высокого уровня критичности, что влечет за собой нервозность и требовательность заказчиков, а также различные технологические сложности, которые приходится исправлять в кратчайшие сроки.

Один из возможных путей решения назревших проблем—это внедрение новых технологий, которые снимут часть нагрузки с персонала

SOC в области анализа и обработки инцидентов кибербезопасности. Особенность нового подхода в работе SOC (SOC NG) это не реактивное реагирование на инциденты кибербезопасности, а обеспечение проактивной защиты, которая базируется на анализе ландшафта угроз и прогнозировании возможных угроз для каждой конкретной организации.

Такой анализ и прогнозирование — это обработка больших массивов данных (Big Data), которая предполагает долгосрочное хранение этих данных, использование машинного обучения и искусственного интеллекта. В результате выявляются аномалии, которые помогают выявить скрытые угрозы.

К технологиям, используемым в SOC NG относятся:

— технологии UEBA (User and Entity Behavior Analytics), реализующие анализ поведения пользователей и объектов информационной системы и на основании этого анализа выявляющие возможные угрозы;

— технологии SOAR (Security Orchestration, Automation and Response), обеспечивающие согласованность действий различных элементов системы защиты информации организации, в том числе и эффективное распределение задач среди специалистов SOC. SOAR может быть интегрирована с другими бизнесс-системами организации и использовать их данные для выявления скрытых угроз. Помимо этого, SOAR-платформы могут разрабатывать типовые сценарии реагирования на события кибербезопасности и реализовывать автоматическое реагирование на инциденты кибербезопасности, используя IRP (Incident Response Platforms).

Для обеспечения проактивной защиты необходим сбор информации о потенциальных угрозах кибербезопасности (Threat intelligence). Такая информация позволяет разработать наиболее вероятные сценарии атак на организацию и на основании этих сценариев определить оптимальные пути минимизации рисков от таких угроз.

Для оптимизации работы SOC NG следует выделить в команде три линии специалистов и максимально автоматизировать рутинные задачи. Важным моментом в работе сотрудников первой линии является строгое следование инструкциям, что снижает время обработки инцидента и уменьшает возможность совершения ошибочных действий. Вторая линия обрабатывает инциденты среднего и высокого уровня критичности, которые требуют более глубокого анализа. Третья линия в основном занимается проактивным поиском и изоляцией сложных угроз и скрытой активности, которые не выявили существующие средства защиты [5].

Для эффективного противодействия угрозам необходимо менять тактику и методы защиты информации, использовать новые технологии. При модернизации SOC, следует проанализировать слабые и сильные стороны имеющегося центра. Важным моментом является анализ и оценка имеющегося уровня информационной безопасности в компании, что поможет определить слабые места в системе защиты. Следует также проанализировать последние инциденты в сфере ИБ, чтобы убедиться, что в существующей системе защиты есть средства их обнаружения и реагирования.

Понимание того, в каких областях организация уязвима, поможет определить, какие технологии нужны. Автоматизации является одним из ключевых моментов совершенствования SOC. При автоматической обработке около 30 процентов событий, увеличится эффективность работы персонала, что также спасет людей от выгорания и не подвергнет риску компанию. Выбранная правильная технология снизит объем сигналов, который придется обрабатывать людям, давая им возможность сосредоточиться на проблемах, которые технические средства не могут решить.

Список источников

1. Bryan Palma, CEO of Trellix, “What Is a Security Operations Center (SOC)?” URL: https://www.trellix.com/en-us/security-awareness/operations/what-is-soc.html (дата обращения: 16.05.2023).

2. Security Vision, блог «SOC (Security Operation Center): что это такое и зачем используется? Центры мониторинга информационной безопасности» [Электронный ресурс] URL: https://www.securityvision.ru/blog/soc-chto-eto/ (дата обращения: 16.05.2023).

3. АО «ДиалогНаука»/InformationSecurity, «Актуальные проблемы SOC» [Электронный ресурс] URL: https://www.itsec.ru/articles/aktualnyye-problemy-soc/ (дата обращения: 16.05.2023).

4. SolarJSOC. «Как трансформируется SOC в текущих условиях» [Электронный ресурс] URL: https://safe-surf.ru/specialists/article/ (дата обращения: 16.05.2023)

5. Kaspersky/Anti-Malware&Ngenix, «Концепция создания SOC следующего поколения» [Электронный ресурс] URL: https://www.anti-malware.ru/analytics/Technology_Analysis/Next-Generation-SOC-Concept#part31 (дата обращения: 16.05.2023).

Об авторах

Карелова Оксана Леонидовна—
доктор физико-математических наук, доцент, профессор кафедры международной информационной безопасности Московского государственного лингвистического университета, профессор кафедры прикладных информационных технологий Российской академии народного хозяйства и государственной службы при Президенте РФ (Россия, Москва).
E-mail: okarelova@yandex.ru.

Дробышев Артем Владиславович—
студент 4-го курса (бакалавриат) Московского государственного лингвистического университета (Россия, Москва).
E-mail: 2002temych2002@gmail.com.

About the authors

Oksana L. Karelova—
Doctor of Physical and Mathematical Sciences, Associate Professor, Professor of the Department of International Information Security of the Moscow State Linguistic University, Professor of the Department of Applied Information Technologies of the Russian Presidential Academy of National Economy and Public Administration (Russia, Moscow).
E-mail: okarelova@yandex.ru.

Artem V. Drobyshev—
4th year student (bachelor's degree) Moscow State Linguistic University (Russia, Moscow).
E-mail: 2002temych2002@gmail.com.

УДК 004.056

ПРИМЕНЕНИЕ СИСТЕМ АНАЛИЗА ИСХОДНОГО КОДА В РАЗРАБОТКЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Бочкарев О. И.
Московский государственный лингвистический университет (Россия, Москва)
bo4karyow.oleg@yandex.ru

Научный руководитель:
Гришина Н. В.
Московский государственный лингвистический университет (Россия, Москва)
E-mail: grnat@rambler.ru

Аннотация
Рассматривается важность использования современных анализаторов исходного кода как части модели разработки devops при переходе на методологию devsecops. Это обусловлено необходимостью повышения качества и снижения затрат при разработке программного обеспечения за счет поиска ошибок и уязвимых конструкций в исходном коде на ранних стадиях жизненного цикла продукта.

Ключевые слова
Информационная безопасность, DevOps, DevSecOps, анализ исходного кода, SAST, DAST, IAST.

Для цитирования: Бочкарев О. И. Применение систем анализа исходного кода в разработке программного обеспечения // Hi-Hume Journal.—2023.—№ 1 (1).—С. 24—32.

USE OF SOURCE CODE ANALYSIS SYSTEMS IN SOFTWARE DEVELOPMENT

Oleg I. Bochkarev
Moscow State Linguistic University (Moscow, Russia)
bo4karyow.oleg@yandex.ru

Scientific supervisor:
Natalia V. Grishina
Moscow State Linguistic University (Moscow, Russia)
grnat@rambler.ru

Abstract
The importance of using modern source code analyzers as part of the devops development model when switching to the devsecops methodology is considered. This is due to the need to improve quality and reduce costs in software development by searching for errors and vulnerable structures in the source code at the early stages of the product lifecycle.

Keywords
Information security, DevOps, DevSecOps, source code analysis, SAST, DAST, IAST.

For citation: Bochkarev O. I. Use of source code analysis systems in software development // Hi-Hume Journal.—2023.—№ 1 (1).—Pp. 24—32.

На сегодняшний день вопросам безопасности информации и разработки безопасного ПО уделяется особое внимание, начиная с вузовской подготовки специалистов [1]. В связи с растущими требованиями к качеству продукта разработки, скорости поставок нового функционала конечным пользователям, минимизации издержек и постоянно изменяющимися требованиями заказчика к продукту команды начинают применять гибкие методологии разработки ПО. Применение таких методологий помогает более эффективно осуществлять разработку, а также открывает возможности для улучшения информационной безопасности продукта на ранних этапах его реализации.

В настоящее время актуальными подходами к разработке программного обеспечения считаются каскадный (Waterfall) и гибкий (Agile). Каскадный подход требует поэтапного утверждения схемы разработки и плана проекта, а также запрещает пересматривать предыдущие этапы или модификации после их утверждения. Несмотря на то, что данный подход считается устаревшим, отдельные компании все еще используют его. По сравнению с каскадным подходом, гибкий подход предполагает общение между заказчиком и проектной командой на каждом этапе разработки. Это позволяет минимизировать риски в процессе производства, а также значительно ускоряет процесс принятия решений [3].

Помимо методологии организации работы в команде, не менее важную роль в разработке продукта занимает скорость поставок кода—частота и регулярность релизов. Данный аспект помогает реализовать методология DevOps. Основная концепция DevOps заключается в постоянном сотрудничестве между командами по разработке, тестированию и эксплуатации программного обеспечения. Основное внимание в этих практиках уделяется обеспечению непрерывной поставке высококачественного программного обеспечения и ускорению процесса разработки, например, за счет автоматизации определенных задач.

Согласно методологии DevOps, процесс создания программных продуктов состоит из восьми этапов, причем в левой части цикла представлены процессы, возможности и инструменты, необходимые для разработки, а в правой—для эксплуатации. К процессам разработки относятся: планирование, разработка кода, сборка и тестирование, а к эксплуатации: релиз, поставка, эксплуатация и мониторинг программного продукта [4]. Последовательность этих этапов называется практикой непрерывной интеграции/непрерывной поставки ПО (Continuous Integration/Continuous Deployment, CI/CD). Данный процесс схематично отображен на рисунке 1.

На каждом этапе проводится оценка безопасности, однако команда по безопасности данных не всегда находится в контакте с командами разработчиков и эксплуатации. Они проверяют программный продукт или его исходный код, но не так регулярно, как он меняется. Это может создать риск выпуска небезопасного продукта.

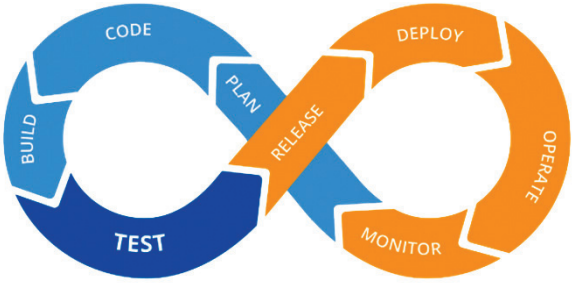

Рис. 1. Принципиальная схема подхода CI/CD

Согласно исследования Национального института стандартов и технологий (NIST), затраты на устранение уязвимостей, обнаруженных после выпуска продукта, могут в тридцать раз превышать расходы на их корректировку на начальных этапах разработки [5]. В связи с этим,

явно прослеживается необходимость включения процессов информационной безопасности на ранних этапах реализации проекта, в целях сокращения материальных и временных издержек, а также повышения качества итогового продукта.

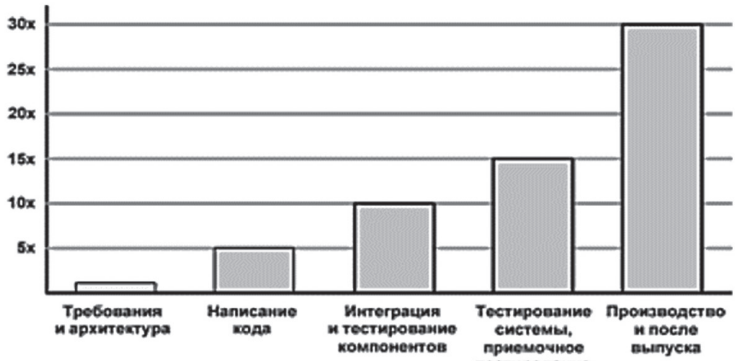

Рис. 2. Относительная стоимость внесения исправлений в продукт в зависимости от времени обнаружения уязвимостей.

Для решения данной задачи появилась методология DevSecOps—это методика интеграции принципов безопасности в конвейер непрерывной интеграции, непрерывной поставки и непрерывного развертывания. Применение на практике принципов DevOps в области безопасности ПО означает, что тесты безопасности являются неотъемлемым элементом процедуры разработки. Это предполагает инициирование процесса обеспечения безопасности на самых ранних этапах планирования разработки ПО, гарантируя, что все команды, участвующие в разработке, тестировании и эксплуатации, знают и выполняют требования безопасности, связанные с продуктом. Такой подход называется «сдвигом влево» (Shift Left) [5].

Основные составляющие методологии DevSecOps

Согласно принципиальной схемы методологии DevOps, существуют восемь этапов непрерывного, замкнутого жизненного цикла продукта. На каждом этапе цикла, мы внедряем элементы безопасности, которые становятся неотъемлемой частью данного цикла. Рассмотрим их подробнее.

- **Планирование (Plan)**—этап планирования является наименее автоматизированным. Здесь происходит обсуждение, тестирование и разработка стратегии безопасности для продукта. Результатом

будет план, описывающий, где, когда и как будет проводиться тестирование безопасности.

- **Разработка (Code)**—на данном этапе подключаются статические анализаторы кода. Этап предполагает автоматизацию процесса, путем подключения инструмента анализа кода непосредственно в рабочий процесс системы контроля версий Git, при котором каждый коммит и слияние веток является триггером на автоматический запуск исследования исходного кода. Такие инструменты поддерживают различные языки программирования и среды разработки.
- **Сборка проекта (Build)**—этап сборки начинается после того, как разработчик направляет свой код в исходный репозиторий, по окончанию работ по исследованию исходного кода. На данном этапе проводится анализ программных компонентов (components analysis), статическое тестирование (SAST). Данный этап также предполагает автоматизацию путем включения в конвейер CI/CD.
- **Тестирование (Test)**—этап тестирования начинается после сборки и успешного развертывания в тестовой среде. На этапе тестирования используются инструменты тестирования безопасности с динамическим анализом (DAST). Они помогают выявить рабочие процессы приложений: аутентификацию пользователей, авторизацию, SQL Injection и конечные точки, связанные с API. DAST-тестирование направлено на обеспечение безопасности и помогает проверить приложение на наличие известных проблем высокой степени опасности (такие проблемы перечислены в списке OWASP Top 10) [6].
- **Релиз (Release)**—к данному этапу цикла приложение и исполняемый файл должны быть тщательно протестированы. На этапе релиза особое внимание уделяется обеспечению безопасности инфраструктуре, среде выполнения продукта разработки. Настраивается доступ пользователей исходя из парадигмы PoLP. Данная парадигма означает, что любой пользователь, программа или процесс имеют лишь минимально необходимый доступ для выполнения своих функций. Сюда относится выполнение аудита ключей API и токенов доступа, для того чтобы ограничить доступ владельцам. Этап предполагает автоматизацию путем использования систем управления конфигурацией.
- **Развертывание (Deploy)**—если предыдущие этапы прошли успешно, выполняется развертывание артефакта сборки в рабочей среде. Однако при запуске продукта в производственной среде

могут возникнуть проблемы с безопасностью. Например, несоответствия конфигурации рабочей среды и средой промежуточного ПО или средой разработки.

- **Поддержка и мониторинг (Operate, Monitor)**—на данном этапе конечные пользователи начинают работу с продуктом. Команда безопасности осуществляет мониторинг работающего приложения на предмет атак и утечек данных.
- **Поддержка и мониторинг (Operate, Monitor)**—на этом этапе конечные пользователи начинают работу с продуктом. Команда безопасности осуществляет мониторинг работающего приложения на предмет атак и утечек данных.

Как было отмечено ранее, чем раньше в проекте будут обнаружены уязвимости, тем меньше издержек мы получим. Поэтому крайне важно на ранних этапах применять инструменты анализа исходного кода, и включать их в процесс CI/CD в автоматическом режиме. Это не освободит от дальнейшего участия команды безопасности в цикле разработки, но позволит минимизировать затраты и конечную стоимость продукта в будущем.

Элементы DevSecOps переносят задачу на более раннюю стадию цикла разработки. Сдвиг безопасности «влево» гарантирует соблюдение стандартов безопасности с момента первой разработки кодовой базы. Задачи разработки считаются выполненными не только тогда, когда выполняются функциональные требования, но и когда кодовая база проверяется на отсутствие недостатков и уязвимостей безопасности [5].

Непрерывная система обратной связи обеспечивается автоматизированным механизмом, который отслеживает угрозы безопасности в момент публикации исходного кода в репозитории и предупреждает об этом разработчиков и ответственных специалистов. Регулярный анализ помогает членам команды продолжать совершенствовать свою деятельность по разработке и поддержанию системы.

Автоматизация является ключевым фактором в соблюдении стандартов и практик DevSecOps на всех этапах жизненного цикла разработки. Автоматизация позволяет командам DevSecOps быстро брать на себя дополнительные обязанности по обеспечению безопасности, включая автоматический анализ кода, мониторинг соответствия и расследование угроз.

Трудности при внедрении методологии DevSecOps

1. Внедрение новых методологий приводит к изменению условий труда и привычного уклада. Для людей является естественным сопротив-

ление смене состояния или процесса. Командам, которые традиционно работали независимо друг от друга, может быть трудно приспособиться к новой модели devsecops, предусматривающей сотрудничество между отделами. Чтобы сделать переход как можно более плавным, важно заручиться поддержкой заинтересованных сторон и четко описать преимущества перехода. При планировании перехода на devsecops организовать вместе руководство и членов команд разработки, безопасности и эксплуатации, чтобы учесть потребности и приоритеты каждого. Это даст всем возможность обозначить свои потребности, снизить напряжение между командами, и найти решения, закрывающие потребности всех стейкхолдеров.

2. DevSecOps методология требует новых инструментов и процессов, которые ранее не применялись. Некоторые из уже используемых инструментов и процессов внутри команд могут оставаться полезными после перехода [2]. Остальные необходимо переоборудовать или заменить. Интеграция инструментов тестирования безопасности обычно является отправной точкой, например, инструменты статического (SAST) и динамического (DAST) тестирования безопасности приложений могут использоваться на протяжении всего процесса разработки. Если инструмент сложен в использовании или замедляет производительность, он будет мешать организационным изменениям. Инструменты и процессы должны быть интегрированы и хорошо работать для всех участников. Они также должны быть направлены на максимальную автоматизацию рабочего процесса, чтобы сделать совместную работу более простой и продуктивной.

3. Разработчики не специалисты по безопасности. Новая методология предполагает, что группы эксплуатации и разработки разделяют обязанности по обеспечению безопасности. Может возникнуть напряженность между потребностью в скорости и потребностью в безопасности. Важно найти баланс между этими двумя вещами. Сложность процесса и требований безопасности представляет собой определённую трудность, потому что тем, кто разрабатывает продукт, надо освоить расширенный перечень методов безопасного программирования. Также им приходится непосредственно включать тестирование безопасности в свою повседневную работу. Это необходимо, хотя и существенно замедляет скорость работы, по крайней мере поначалу [7].

Выводы

Включение современных анализаторов исходного кода в процесс разработки и переход к методологии DevSecOps позволит повысить ка-

чество и снизить издержки в процессе разработки программных продуктов путем нахождения ошибок и уязвимых конструкций в исходном коде на ранних этапах жизненного цикла продукта.

Чтобы свести к минимуму проблемы при переходе на новую методологию необходимо проводить обучение по вопросам безопасности для всех участников проекта внедрения. Обучение должно информировать участников, не связанных с безопасностью, о лучших практиках безопасности и их важности, а также обучать команды безопасности инструментам и методам DevSecOps. Общение и сотрудничество являются ключевыми факторами в данном процессе.

Автоматизация поможет разработчикам меньше беспокоиться о новых процессах, и они смогут сосредоточиться на написании кода. Обдуманный выбор и использование инструментов автоматизации, интеграция информации о безопасности и предупреждений в среду разработки может помочь исполнителям освоить навыки безопасного кода.

Список источников

1. Былевский П. Г. Некоторые особенности интеграции инновационных технологий и методик в высшее гуманитарное образование / Инновационные технологии обучения в вузах. Сборник статей национальной научно-практической конференции.—Сочи – Москва: ОЧУ ВО «Московский инновационный университет», 2022.—С. 40-45.

2. Максимовский А. Ю., Мельников С. Ю. Спектральные и комбинаторные свойства редуцированных графов де Брейна // Вопросы кибербезопасности.—2018. № 4 (28).—С. 70-76.

3. Шляпкин А. В. Метод оценки экономической эффективности подразделения по защите информации // Информационные системы и технологии: управление и безопасность.—2014.—№3.—С. 318-324.

4. DevOps методология.URL: [Электронный ресурс] https://www.tadviser.ru/index.php/Статья:DevOps_Методология (Дата обращения: 06.06.2023).

5. Souppaya M., Scarfone K., Dodson D. NIST SP 800-218 “Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities” [Электронный ресурс] UR: https://csrc.nist.gov/publications/detail/sp/800-218/final (Дата обращения: 06.06.2023).

6. OWASP Top Ten Foundation. [Электронный ресурс] URL: https://owasp.org/www-project-top-ten (Дата обращения: 06.06.2023).

7. Флорен М. В. Организация управления доступом // Защита информации. — Конфидент. — 1995. — № 5. — С. 87–93.

Об авторах

Бочкарев Олег Игоревич —
студент 2-го курса (магистратура)
Московского государственного
лингвистического университета
(Россия, Москва).
E-mail: bo4karyow.oleg@yandex.ru.

Гришина Наталья Васильевна —
кандидат технических наук, доцент,
доцент кафедры информационной
культуры цифровой трансформации
Института информационных наук
Московского государственного
лингвистического университета
(Россия, Москва).
E-mail: grnat@rambler.ru.

About the authors

Oleg I. Bochkarev —
2nd year student (Master's degree)
Moscow State Linguistic University
(Russia, Moscow).
E-mail: bo4karyow.oleg@yandex.ru.

Natalia V. Grishina —
Candidate of Technical Sciences,
Associate Professor, Associate Professor
of the Department of Information
Culture of Digital Transformation of the
Institute of Information Sciences
of the Moscow State Linguistic
University
(Russia, Moscow).
E-mail: grnat@rambler.ru.

УДК 004.056

СРАВНИТЕЛЬНЫЙ АНАЛИЗ SIEM-СИСТЕМ НА РОССИЙСКОМ РЫНКЕ

Кривошапка П. Г.
Московский государственный лингвистический университет (Россия, Москва)
polia.kr@yandex.ru

Научный руководитель
Былевский П. Г.
Московский государственный лингвистический университет (Россия, Москва)
pr-911@yandex.ru

Аннотация
В статье проводится сравнительный анализ доступных на российском рынке систем класса SIEM, выявляются их основные функции, достоинства и недостатки.

Ключевые слова
SIEM, информационная безопасность, кибербезопасность, инцидент, событие.

Для цитирования: Кривошапка П. Г. Сравнительный анализ SIEM-систем на российском рынке // Hi-Hume Journal.—2023.—№ 1 (1).—С.33 – 38.

COMPARATIVE ANALYSIS OF SIEM SYSTEMS ON THE RUSSIAN MARKET

Polina G. Krivoshapka
Moscow State Linguistic University (Russia, Moscow)
polia.kr@yandex.ru

Scientific supervisor
Pavel G. Bylevskiy
Moscow State Linguistic University (Russia, Moscow)
pr-911@yandex.ru

Abstract

The article provides a comparative analysis of SIEM class systems available on the Russian market, identifies their main functions, advantages and disadvantages.

Keywords

SIEM, information security,cybersecurity, incident, event.

For citation: Krivoshapka P. G. Comparative analysis of SIEM systems on the Russian market// Hi-Hume Journal.—2023.—№ 1 (1).—Pp. 33—38.

В связи с ограниченным присутствием иностранных вендоров на российском рынке информационной безопасности, а также в соответствии с Указом № 250 "О дополнительных мерах по обеспечению информационной безопасности Российской Федерации" [1], который устанавливает запрет на использование с 1 января 2025 года средств защиты информации, произведенных в недружественных государствах (либо производителями которых являются организации, находящиеся под их юрисдикцией, подконтрольные им, либо аффилированные с ними), возникает потребность в анализе доступных SIEM систем как критически важного компонента обеспечения информационной безопасности организации, включая анализ пользовательских и персональных данных [2].

Системы класса SIEM(Security Information and Event Management) отвечают за мониторинг событий по безопасности, расследование инцидентов и реагирование на них, обнаружение угроз (в том числе благодаря использованию ретроспективного анализа), обеспечивают подтверждение соответствия требованиям и предоставление отчётов об этом. Кроме того, системы этого класса предоставляют аналитику в целях реагирования на инциденты, способствуют поиску угроз [3] и автоматизации рабочих процессов и выполнения задач. SIEM-системы первого поколения в целях решения поставленных задач выполняют агрегацию, корреляцию, нормализацию, фильтрацию, классификацию и приоритезацию событий.

Системы следующего поколения обеспечивают также анализ событий, инцидентов и их последствий, а также принятие решений и визуализацию. К основным функциям SIEM, как правило, относят сбор в центральный репозиторий информации о событиях по различным источникам, где она обрабатывается и хранится в различных формах в

целях дальнейшего анализа этой информации, создания отчетов на ее основе и обеспечения возможного ретроспективного анализа данных для криминалистической экспертизы и выявления угроз [4].

В данной статье будут рассмотрены следующие SIEM системы: RuSIEM компании ООО «РуСИЕМ», Kaspersky Unified Monitoring and Analysis Platform (KUMA) от АО «Лаборатория Касперского», KOMRAD Enterprise SIEM от компании АО «НПО «Эшелон», MaxPatrol SIEM от компании АО "ПОЗИТИВ ТЕКНОЛОДЖИЗ".

1. Kaspersky Unified Monitoring and Analysis Platform.

На основе руководства по эксплуатации, а также схожих материалов, представленных на сайте производителя можно выделить следующие преимущества [5]:

- обеспечение централизованного рабочего пространства специалиста для выявления угроз, анализа и реагирования на них за счёт
- интеграция с другими продуктами производителя, а также возможность интеграции сторонних продуктов, например, VM-сканеров и SOAR-системы, что в свою очередь позволяет реализовать концепцию XDR;
- наличие высокопроизводительной, горизонтально масштабируемой БД ClickHouse, поддерживающей компрессию данных;
- высокая производительность (свыше 300 000 EPS) на один узел системы (коррелляторы, базы данных и т. д.);
- возможность интеграции с платформой Kaspersky CyberTrace для агрегации данных об угрозах;
- возможность интеграции с Kaspersky Security Center для автоматической инвентаризации активов.

2. MaxPatrol SIEM

Согласно представленному на сайте производителя описанию [6] MaxPatrol SIEM, к преимуществам данного продукта можно отнести:

- регулярное получение специальной информации о новых методах проведения атак и о способах выявления самых актуальных угроз;
- специальную технологию управления активами (SecurityAssetManagement), которая позволяет автоматизировать процесс сбора подробной информации о каждом IT-активе;
- процесс развертывания и эксплуатации программного обеспечения сопровожден интуитивно понятным пользовательским интерфейсом, кроме того, предоставляется обучение специалистов на базе собственного учебного центра;

- возможность интеграции с большим количеством систем для сбора сведений;
- возможность подключения любых бизнес-систем, в том числе специфических и самописных;
- гибкий язык описания логики работы правил корреляции для задач различных уровней сложности.

Также необходимо отметить активоцентрическую модель, которая, в том числе позволяет лицензировать продукт не по потоку событий, а по количеству активов, то есть, независимо от объема получаемых данных из источников и от изменения количества событий в секунду.

3. KOMRAD Enterprise SIEM

К преимуществам KOMRAD Enterprise SIEM можноотнести [7]:

- относительно высокую производительность при низких требованиях к аппаратному обеспечению;
- визуальный графический интерфейс для создания фильтров и правил корреляции; управление инцидентами;
- возможность распределённой установки и масштабирования;
- интеграцию со всеми отечественными СЗИ, в том числе с API ГосСОПКА;
- передачу инцидентов в формате CEF в другие системы;

4. RuSIEM

На основе представленных на сайте производителя данных, к преимуществам данной системы можно отнести:

- гибкие корреляционные правила с применением современных аналитических подходов;
- универсальные коннекторы подключения новых источников;
- модульные варианты развёртывания длянизкобюджетных конфигураций;
- неограниченное горизонтальное и вертикальное масштабирование;
- встроенный инцидент-менеджмент;
- обеспечение получения всех событий без потерь вне зависимости от протокола передачи [8].

В *Таблице 1* представлены характеристики, которые дополнительно следует учесть при выборе систем для внедрения и использования в рамках построения системы защиты информации организации.

Таблица 1. Сравнительные характеристики SIEM-систем

	Kaspersky KUMA	**KOMRAD Enterprise SIEM**	**MaxPatrol SIEM**	**RuSIEM**
Общая интегрируемость	Высокая	Высокая	Высокая	Средняя
Обучение специалистов администрированию системы	Есть	Есть	Есть	Есть
Наличие встроенного сканера уязвимостей	Отсутствует / не заявлен	Есть	Есть	Есть
Интеграция со сканерами уязвимостей	Отсутствует / не заявлен	Отсутствует / не заявлен	Есть	Отсутствует/ не заявлен
Конструктор правил корреляции	Есть	Есть	Есть	Отсутствует / не заявлен
Ретроспективный анализ	Есть	Отсутствует / не заявлен	Есть	Отсутствует / не заявлен
Среды функционирования	Microsoft Windows Server2012 R2; 2016; 2019. Microsoft Windows 10 (20H1, 20H2, 21H1). Ubuntu 20.04 LTS, 21.04. Oracle Linux 8.4.	Astra Linux Special Edition 1.6, Debian 7, Ubuntu 20, ОСОН «ОСнова» 2	Astra Linux Special Edition 1.7; Debian 10; Microsoft Windows Server 2012, 2012 R2, 2016; 2019	Ubuntu 18.04×64

В заключение необходимо отметить, что подбор комплексных программных решений класса SIEM должен производиться с учетом ряда исходных параметров информационной системы организации, а также дальнейшего развития информационной системы, экономического обоснования и юридических требований для данной организации.

Список источников

1. Указ Президента Российской Федерации от 01.05.2022 № 250 "О дополнительных мерах по обеспечению информационной безопасности Российской Федерации" [Электронный ресурс] URL:http://www.kremlin.ru/acts/bank/47796 (дата обращения 20.11.2022).

2. Былевский П. Г. Пользовательские и персональные данные: анализ рисков «извлечения знаний» // Вопросы защиты информации.—2023. № 1—(140).—С. 35-40.

3. Кириллов В. А., Касимова А. Р., Алёхин А. Д. Система сбора и корреляции событий (siem) как ядро системы информационной безопасности // Вестник технологического университета.—2016.—Т.19.—№13.—С. 132-134.

4. Германович А. В., Мельников С. Ю., Пересыпкин В. А., Сидоров Е. С., Цопкало Н. Н. Информационные измерения языка. Программная система оценки читаемости искаженных текстов // Известия ЮФУ. Технические науки.—2019.—№ 7 (209).—С. 6-17.

5. Руководство по эксплуатации Kaspersky Unified Monitoringand Analysis Platform. [Электронный ресурс] URL: https://builds-by.kaspersky.ru/uploads/KUMA/KUMA 1.5 Руководство по эксплуатации.pdf (дата обращения 25.11.2022).

6. MaxPatrol SIEM. [Электронный ресурс] URL: https://www.ptsecurity.com/upload/ptru/products/documents/mpsiem/PT-MaxPatrol-SIEM-Product-Brief-rus.pdf (дата обращения 29.11.2022).

7. KOMRAD Enterprise SIEM. [Электронный ресурс] URL: https://npoechelon.ru/production/65/11793 (дата обращения 25.11.2022).

8. RuSIEM. [Электронный ресурс] URL: https://rusiem.com/ru/company/pressroom/articles/obzor-rusiem-33-otechestvennoj-siem-sistemy (дата обращения 25.11.2022).

Об авторах

Кривошапка Полина Георгиевна—
студент 4 курса (бакалавриат)
Института информационных наук
Московского государственного
лингвистического университета
(Россия, Москва).
E-mail: polia.kr@yandex.ru.

Былевский Павел Геннадиевич—
кандидат философских наук, доцент;
Московский государственный
лингвистический университет
(Россия, Москва). E-mail: pr-911@yandex.ru.

About the authors

Polina G. Krivoshapka —
4th year student (bachelor's degree)
Institute of Information Sciences of
the Moscow State Linguistic University
(Russia, Moscow).
E-mail: polia.kr@yandex.ru.

Pavel G. Bylevskiy —
Candidate of Philosophical Sciences,
Associate Professor; Moscow State
Linguistic University (Russia, Moscow).
E-mail: pr-911@yandex.ru.

УДК 004.056

ОСОБЕННОСТИ И ПРЕИМУЩЕСТВА ВНЕДРЕНИЯ ТЕХНОЛОГИЙ БЛОКЧЕЙН В ГОСУДАРСТВЕННЫХ ОРГАНИЗАЦИЯХ

Гусев В. С.
Московский государственный лингвистический университет (Россия, Москва)
bear.01@bk.ru

Былевский П. Г.
Московский государственный лингвистический университет (Россия, Москва)
pr-911@yandex.ru

Аннотация

В современном мире развитие технологий происходит настолько быстро, что для специалистов по информационной безопасности крайне важно успевать адаптироваться. Технологии блокчейн позволяют надёжно защищать информацию, добиться прозрачности операций, а также ускорить и оптимизировать сам процесс работы государственного сектора. Данная статья предназначена для изучения принципа работы технологии блокчейн и преимуществ его внедрения на государственном уровне.

Ключевые слова

Информационная безопасность, блокчейн, государственный сектор, оптимизировать процесс работы.

Для цитирования: Гусев В. С. Особенности и преимущества внедрения технологий блокчейн в государственных организациях // Hi-Hume Journal.—2023.—№ 1 (1).—С. 39—47.

FEATURES AND ADVANTAGES OF TECHNOLOGY IMPLEMENTATION BLOCKCHAIN IN GOVERNMENT ORGANIZATIONS

Vadim S. Gusev
Moscow State Linguistic University (Moscow, Russia)
bear.01@bk.ru

Scientific supervisor
Pavel G. Bylevsky
Moscow State Linguistic University (Russia, Moscow)
pr-911@yandex.ru

Abstract
In the modern world, the development of technologies is happening really fast and it is extremely important for information security specialists to be ready for adapting. Blockchain technologies are able to provide reliable protection of information, achieve transparency of operations, speed up and optimize the process of the public sector operations. This article is intended to study the principle of blockchain technology and the advantages of its integration in the state level.

Keywords
Information security, blockchain, public sector, to optimize the process.

For citation: Gusev V. S. Features and advantages of the introduction of blockchain technologies in government organizations // Hi-Hume Journal.—2023.—№ 1 (1).—Pp. 39—47.

Введение

В современном мире технологии постоянно развиваются, что делает очень важным умение и возможность адаптироваться к ним и находить для них эффективное применение в обычной жизни людей. Решение вопросов информационной безопасности систем организаций и баз данных сегодня является особенно актуальным, включая использование новейших высокотехнологичных средств [3]. Это относится не только к частным организациям, защищающим свои активы от недобросовестных конкурентов, но также затрагивает и государственный сектор, в котором последствия утраты конфиденциальности, целостности и доступности информации могут быть гораздо серьёзнее [5].

В нынешних условиях справиться с решением данных вопросов, поможет внедрение технологии блокчейн и использование смарт-контрактов в работу государственных организаций. Блокчейн—относительно новая технология, интерес к которой вырос вместе с популярностью криптовалют. Однако сегодня ее не только широко обсуждают в финансовой отрасли, но уже активно начинают использовать для

хранения и обработки персональных данных и идентификации пользователей во многих жизненных сферах, в том числе в сфере недвижимости.

Идея данной технологии впервые была описана двумя исследователями в 1991 году, когда ученые Стюарт Хабер и У. Скотт Шторнетт внедрили вычислительно-практическое решение для цифровых документов с штампом времени, чтобы они не могли быть подделаны или оформлены с указанием неправильной даты. Система использовала криптографически закрепленную цепочку блоков, для хранения документов с отметкой времени, а в 1992 году деревья Меркла были включены в разработку, что дало развитие данной технологии и сделало её более эффективной, позволив собирать несколько документов в один блок. Однако эта технология не использовалась, и патент был упущен в 2004 году, за четыре года до создания самой известной криптовалюты в мире—биткойна [6].

Децентрализация и прозрачность блокчейна значительно снижает вероятность фальсификации баз данных. Обычно у злоумышленника удается заполучить информацию при атаке основного места хранения данных—сервера. В блокчейне это практически невозможно, потому что вся информация хранится распределенно по сети блокчейн, а потому для хакеров не существует необходимого направления атаки. Им потребуется повредить одни и те же данные во всех блоках. Так как каждое изменение в блокчейне становится заметным всем его пользователям, при этом оно также должно быть утверждено их большинством, то такая атака требует слишком больших ресурсов в виде компьютерных вычислительных мощностей, что делает ее невыгодной и сложной для выполнения.

Таким образом, блокчейн способен защитить данные и оптимизировать процессы работы с ними.

Принцип работы технологии блокчейн

Для начала необходимо разобраться что такое блокчейн, как он работает и как используются смарт-контракты. Блокчейн—это непрерывная цепочка блоков, в которой содержатся все записи о транзакциях. Однако изменить или удалить эти записи нельзя, имеется возможность только добавить новые, в отличие от обычных баз данных.

Блокчейн также называют технологией распределенных реестров, потому что всю цепочку сделок и актуальный список владельцев хранят на своих компьютерах множество независимых пользователей. Даже если один или несколько компьютеров, выступающих в роли серверов,

дадут сбой, информация не пропадет, пока будет работать хотя бы один компьютер при наличии доступа в интернет. Конечно, в таком случае производительность самого блокчейна значительно ухудшится, но потери данных удастся избежат [1].

Записи транзакций, находящихся на определенном блокчейне, находятся в открытом доступе для всех его пользователей. Это означает, что информация о всех транзакциях будет открытой и любой человек сможет увидеть полную информацию. Публичная сеть имеет преимущество, потому что все ее данные находятся в поле зрения общественности. При достаточном внимательном наблюдении за блокчейном появляется возможность обнаружить, выявить и отследить любое изменение, сделанное в ней, что делает вероятность появления незамеченных изменений близкой к нулю.

При вводе информации в блокчейн происходит хеширование—преобразование информации с помощью криптографических функций. Это означает ввод информации любой длины и размера в исходной строке и выдачу результата фиксированной длины заданной алгоритмом функции хэширования. Небольшие изменения в вводимых данных изменяют хэш.

При внесении даже небольших изменений в исходные данные, изменения, которые будут отражены в полученном значении хеширования (набора символов определённой алгоритмом длины), будут огромными, что значительно повышает сложность обратного вычисления.

Кроме того, благодаря хешированию, когда строка данных добавляется или изменяется, новая запись и предыдущая запись остаются видимыми, так как ни одна из них не может быть удалена. Таким образом, это позволяет отследить все изменения, внесенные злоумышленниками. В этом случае преступник должен будет незаметно войти в сеть блокчейн, сделать определённые действия с информацией и незаметно уйти. Учитывая сложность доступа к каждому блоку данная атака становится практически невыполнимой из-за количества необходимых для этого ресурсов.

История создания и принцип работы смарт-контрактов

Смарт-контракты—это алгоритм определенных действий, интегрированный в код блокчейна. При соблюдении установленных договоренностей, которые в нем прописаны, выполняется автоматический запуск данной последовательности. Сам алгоритм прописан внутри блокчейна, поэтому правила осуществления условий сделки не поддаются изменению и являются обязательными для всех участников.

Самое первое упоминание о цифровых договорах появилось еще в 1996 году. Ник Сабо, американский ученый в сфере криптографии, предложил использовать подобие смарт-контрактов. В то время идея была слишком футуристична и не получила должного признания. Полностью концепт его идеи об "умных контрактах" был реализован в 2013 году на блокчейне Ethereum, в основу которого легла современная технология смарт-контрактов. Он позволял разрабатывать и запускать приложения без новых распределительных реестров.

Смарт-контракты являются частью программного кода блокчейна и работают непосредственно внутри сети. Они выполняют функцию бумажных договоров, только в цифровом поле. Условия прописываются не ручкой на бумаге, а с применением математических алгоритмов и языков программирования. Как и в бумажном договоре, условия подлежат обязательному выполнению. Только в таком случае сделка будет реализована и пользователи получат обусловленный результат. После завершения алгоритма и корректного проведения операции, смарт-контракты становятся частью реестра, попадая в саму цепочку блоков блокчейна.

Главный принцип смарт-контракта—абсолютно полное исполнение обусловленного алгоритма последовательных действий, который был задан при его создании. Смарт-контракты получили активное распространение по всему миру, так они позволяют оптимизировать и ускорить множество рутинных процессов и снизить (или полностью исключить) участие посреднической стороны, что существенно уменьшает связанные с этим расходы. Увеличение использования технологии смарт-контрактов также обусловлено тем, что данная технология предоставляет возможность исключить ошибки, которые были возможны из-за человеческого фактора.

Преимущества внедрения технологии блокчейн

Существует несколько главных преимуществ внедрения блокчейна в государственный сектор [4]: децентрализация, защищённость, прозрачность и высокую скорость транзакций. Прозрачность блокчейна позволяет решить серьезную проблему коррупции, так как данная технология предоставляет гражданам возможность видеть все происходящие транзакции. В таком случае не будет возможности совершать незаконные операции по распределению бюджета.

Это позволит поднять доверие людей, отслеживать движение бюджетных средств и выявлять ответственных за преступления коррупционеров. Высокая скорость и защищенность транзакций позволяет

государствам создать собственную цифровую валюту. Использование смарт-контрактов также позволит сразу высчитывать и забирать необходимую сумму налогообложения, например при получении заработной платы.

Смарт-контракты могут использоваться для получения персональных документов, таких как паспорт, право на собственность или диплом об образовании, которые будут закреплены в блокчейне. Это оптимизирует и значительно облегчит процесс документооборота, так как утрата документа станет невозможной и вся необходимая информация будет находиться в блокчейне.

А также интеграция технологий блокчейна на основе смарт-контрактов сможет обеспечить максимальную объективность выборов и честно оценивать голоса избирателей. Использование данных технологий сможет решить многие проблемы во время избирательных процессов. Их нельзя изменить, нарушить или пренебречь алгоритмом в свою пользу. Поэтому у людей появится больше уверенности в прозрачности и необходимости участия в выборах.

Особенности внедрения технологии блокчейн

Несмотря на большое количество преимуществ внедрения блокчейна в государственную систему, для осуществления данного процесса существуют некоторые трудности и особенности.

Самым важным и сложным моментом является формирование законного обеспечения интеграции блокчейна. Для юридической силы смарт-контрактов требуется большое количество нормативно-правовых актов, которые смогут регулировать процессы, происходящие с помощью блокчейна.

Отдельной проработки заслуживает механизм консенсуса в принятии решения несколькими субъектами государственного управления — например, в случае перевода на блокчейн разрешительной функции, когда для вынесения окончательного решения по выдаче разрешения требуется согласие нескольких субъектов. В этом случае может оказаться полезной разработка типовых соглашений государственных органов об участии в блокчейне.

Нужно также учитывать, что все участвующие в системе органы должны быть предварительно введены в качестве участников в систему блокчейна, а для него нужно юридическое основание.

Учитывая достаточную готовность общества и государства к проблематике блокчейна, можно утверждать, что правовое обеспечение государственного управления способно адаптировать технологию

блокчейна к сложившейся правовой системе. Однако на первых этапах внедрения не исключено возникновение определенных проблем.

Примеры использования блокчейна и смарт-контрактов в современных условиях

Одним из примеров успешной интеграции технологии смарт-контрактов в сфере поставок стал цифровой договор между авиакомпанией S7 и Газпромнефть-Аэро. Умный контракт на предмет заправки воздушного транспорта позволил полностью автоматизировать процессы планирования поставки горючего и сопутствующие расчеты.

Центральный банк Аргентины совместно с крупными коммерческими банками начал тестировать новую клиринговую систему на основе сети смарт-контрактов, что позволит ускорить расчеты. Решение работает на управляемом блокчейне. Блокчейн-система будет обрабатывать прямые дебетовые транзакции, в которых платеж инициирует не отправитель, а получатель средств. Платформа позволит отслеживать претензии между участниками благодаря децентрализованной корпоративной сети — это облегчит обмен сообщениями и сделает процесс прозрачным.

В 2017 году Грузия была первой страной, которая внедрила революционную технологию блокчейн в государственном секторе и в частности, в государственных сервисах. Грузия запустила пилотную версию земельного кадастра на основе блокчейна. В планах было создание частного блокчейна для регистрации прав собственности, привязанного к блокчейну биткойна.

Это означает, что договора о передаче прав собственности на землю будут заключаться в закрытой системе, таким образом, каждая отдельная транзакция не будет публичной и отслеживаемой, но гарантия неизменности данных сохранится в силу того, что блоки данных и транзакций впоследствии будут регистрироваться в блокчейне биткойна. До этого процесс покупки или продажи земли в Грузии занимал один день. Для регистрации сделки продавцу или покупателю необходимо было обратиться в регистрационную палату и заплатить от 50 до 200$, в зависимости от пожеланий по срокам регистрации. Пилотный проект предлагал перенести часть процесса регистрации в блокчейн, сократив расходы граждан до 0,5—1$.

Заключение

В данной статье были разобраны принципы работы технологии блокчейн и смарт-контрактов, рассмотрены преимущества внедрения

блокчейна в работу государственного сектора. Также были выявлены проблемы, с которыми нам предстоит столкнуться во время интеграции блокчейна и которые предстоит решить. Основываясь на полученной информации можно сделать вывод, что блокчейн с интеграцией смарт-контрактов позволяет создать единую информационную базу с возможностью полной автоматизации процессов передачи и согласования данных, в том числе конфиденциальных, а также исключения ошибок из-за человеческого фактора. Также благодаря своим преимуществам, данная технология позволит победить коррупцию и поднять доверие людей к государству.

Технология блокчейн с каждым днём всё ближе к массовому принятию и использованию, так что необходимо погружаться в нее. Однако необходимо понимать, что внедрение блокчейна приведёт к большим и серьезным изменениям. Скорее всего успешная интеграция данной технологии потребует массовой смены формата работы и создание большой и сложной системы. Однозначно необходимо не только добавить базовое обучение по блокчейну в школьные и университетские программы обучения [2], но и распространять эти знания среди взрослого поколения, так как переход на использование блокчейна приведет к оптимизации многих процессов и к сокращению требуемых человеческих ресурсов. Так что данные знания позволят работникам государственной сферы переквалифицироваться и быть готовым к масштабным изменениям.

Список источников

1. Антонопулос А. М. Интернет денег. — М.: Олимп-Бизнес, 2018. — 180 с.

2. Былевский П. Г. Некоторые особенности интеграции инновационных технологий и методик в высшее гуманитарное образование / Инновационные технологии обучения в вузах. Сборник статей национальной научно-практической конференции. Сочи-Москва, 2022. — С. 40-45.

3. Германович А. В., Мельников С. Ю., Пересыпкин В. А., Сидоров Е. С., Цопкало Н. Н. Информационные измерения языка. Программная система оценки читаемости искаженных текстов // Известия ЮФУ. Технические науки. — 2019. — № 7 (209). — С. — 6-17.

4. Волкова Т. Г. Причины и особенности внедрения технологии блокчейн в пенсионную систему // Вестник Удмуртского университета. — 2020. — Т.30. — Вып. 3. — С. 333—339.

5. Талапина И. В. Применение блокчейна в государственном управлении: перспективы правового регулирования // Вопросы государственного и муниципального управления.— 2020.— № 3.—С. 96—113.

6. Maxat K. Blockchain and e-government innovation: Automation of public information processes // Information Systems.—2022.—Vo. 103.—11 p.

Об авторах

Гусев Вадим Сергеевич—
студент 4 курса (бакалавриат) Института информационных наук Московского государственного лингвистического университета
(Россия, Москва).
E-mail: bear.01@bk.ru.

Былевский Павел Геннадиевич—
кандидат философских наук, доцент; Московский государственный лингвистический университет
(Россия, Москва).
E-mail: pr-911@yandex.ru.

About the authors

Vadim S. Gusev—
4th year student (bachelor's degree) Institute of Information Sciences of the Moscow State Linguistic University
(Russia, Moscow).
E-mail: bear.01@bk.ru.

Pavel G. Bylevskiy —
Candidate of Philosophical Sciences, Associate Professor; Moscow State Linguistic University
(Russia, Moscow).
E-mail: pr-911@yandex.ru.

УДК 316.4

ИМПОРТОНЕЗАВИСИМОСТЬ ОТ ИНОСТРАННЫХ СРЕДСТВ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ: ЭТИКО-СОЦИАЛЬНЫЙ АСПЕКТ

Гостев А. Н.
Московский государственный лингвистический университет, Москва, РФ
Gostevan@inbox.ru

Аннотация

В статье предлагаются пути разрешении проблемы отечественной импортонезависимости информационных ресурсов; аргументируются необходимость ее обеспечения средствами этической социальной инженерии; представляются результаты изучения мнений и настроений управленческих кадров методами экспертного опроса, анализа документов; обосновываются основные пути совершенствования системы обеспечения импортонезависимости на основе этики социальной инженерии.

Ключевые слова

Этическая социальная инженерия, обеспечение импортонезависимости, информационные технологии, социологическое исследование, показатели эффективности социальной инженерии.

Для цитирования: Гостев А. Н. Импортонезависимость от иностранных средств информационных технологий: этико-социальный аспект // Hi-Hume Journal.—2023.—№ 1 (1).—С. 48—60.

IMPORT DEPENDENCE ON FOREIGN MEANS OF INFORMATION TECHNOLOGY: ETHICAL AND SOCIAL ASPECT

Alexander N. Gostev
Moscow State Linguistic University (Moscow, Russia)
Gostevan@inbox.ru

Abstract

The article proposes ways to solve the problem of domestic import independence of information resources; the need to provide it with the means of ethical social engineering is argued; the results of studying the opinions and moods of managerial personnel by methods of expert survey, analysis of documents are presented; the main ways of improving the system of ensuring import independence on the basis of the ethics of social engineering are substantiated.

Keywords

Ethical social engineering, ensuring import independence, information technology, sociological research, indicators of the effectiveness of social engineering.

For citation: Gostev A. N. Import dependence on foreign means of information technology: ethical and social aspect // Hi-Hume Journal. — 2023. — № 1 (1). — Pp. 48—60.

Статья публикуется в контексте изучения дисциплины «Обеспечение импортонезависимости национальной ИКТ-инфраструктуры» и выполнения магистерских диссертаций на кафедре информационной культуры цифровой трансформации Института информационных наук Московского государственного лингвистического университета.

Введение

Импортонезависимость экономики — одна из основ обеспечения национальной безопасности. В этой связи в России создана надежная нормативная правовая база, регулирующая деятельность федеральной исполнительной власти в этой сфере.

В контексте информационных коммуникативных технологий (ИКТ) импортонезависимость обеспечивает гарантированную защищённость электронной компонентной базы (ЭКБ), жизненно важной аппаратуры в форс-мажорных ситуациях. Ретроспективный анализ отечественной практики показывает, что наши геополитические противники регулярно пытаются сдерживать развитие России путем введения различных социально-политических, экономических, культурных и других ограничений (санкций). Уровень актуальности рассматриваемой проблемы значительно возрос уже в 2014 году. Задачу в этой сфере деятельности

системы государственного управления определил Президент РФ: «… надо … создавать товары и сервисы мирового стандарта, … чтобы не копировать, а созидать качественно новое, нужно объединение науки и бизнеса» [2].

Основная ценность современного общества—информация. Информационные цифровые технологии в настоящее время обеспечивают практически все общественные коммуникации, поэтому под угрозой оказалось работа всех общественных институтов России, системы государственного управления [4]. Априори, обеспечение импортонезависимости от средств информационных технологий становится жизненно необходимым [6].

В разрешении этой проблемы нельзя обойтись без этической социальной инженерии, задачами которой являются: развитие «совокупности специфических знаний о воздействиях на человека с целью оптимизировать процесс создания, модернизации и воспроизведения новых социальных реальностей» [1], «обеспечение практическая деятельность по преобразованию всех аспектов общественной жизни для успешной адаптации к изменяющимся условиям реальности» [4].

Непосредственно этика в социальной инженерии регламентирует деятельность на высоком уровне качества, прилежности, нравственности, эффективности, производительности, инициативы, организованности. А сама социальная инженерия решает задачу по формированию всего комплекса положительной психологической характеристики личности, коллективов (групп, организаций) людей.

Результаты наблюдения практики показывают, что предметами социальной инженерии являются все элементы классического алгоритма деятельности человека.

Эмпирическое исследование проводилось с 15 апреля по 15 ноября 2022 года. Опрашивались эксперты (N=216 чел.): студенты и преподаватели Московского государственного лингвистического университета (МГЛУ), Московского педагогического государственного университета (МПГУ), слушатели заочного обучения Академии управления МВД РФ, осуществляющие профессиональную деятельность в различных регионах России. Эксперты дали согласие на использования данных в этом научном труде.

Элементы системы этической социальной инженерии в обеспечении отечественной импортонезависимости

Отдельные элементы системы этической социальной инженерии в системе обеспечения отечественной импортонезависимости от ино-

странных средств информационных технологий в контексте социологического объяснения общественных явлений подробно излагались в научных трудах многих российских ученых.

Результаты анализа научных трудов [4, 5, 8] показывают, что этическая социальная инженерия в системе обеспечения отечественной импортонезависимости от иностранных средств информационных технологий становится системообразующим фактором. Это феномен объясняется тем, что формирование компетенций человека в сфере обеспечения импортонезависимости невозможно без воспитания у управленческих кадров патриотизма, прилежности, уверенности в возможности создавать в нашей стране всего спектра элементов информационных технологий.

Опрос экспертов показал, что в среде отечественных управленцев, производителей, пользователей ИКТ наблюдаются значительное количество людей (18,5% + 16,2=34,7%) с пессимистическим настроением, неуверенностью в перспективах обеспечения импортонезависимости от иностранных средств информационных технологий (см. Схему 1).

Схема 1. Мнение экспертов о перспективах обеспечения независимости России от иностранных средств информационных технологий

Свой пессимизм они объясняют такими фактами: номенклатура импорта—это тысячи наименований элементов радиоэлектронной аппаратуры; часть импортных микросхем технологически невозможно

производить без международной кооперации; отказ от микросхем зарубежного производства приведет к отставанию в развитии электроники.

Кроме того, анализ публикаций в сети интернет позволяет утверждать, что пессимизм российских специалистов ИКТ обусловлен тем, что для успешного микроэлектронного производства необходимо наличие: рынка сбыта; производственного оборудования; компетентного персонала; сырья, материалов и «расходников».

Задача отечественного производства продуктов информационной сферы

Между тем, задача отечественного производства продуктов информационной сферы состоит не в создании тождественного (равного по количеству, качеству и стоимости) продукта, а нового, лучшего, не имеющего равного в мире. Результаты наблюдения практики, ретроспективных исследований показывают, что Россия имеет для этого все интеллектуальные, экономические, сырьевые возможности для разработки и производства собственных информационных коммуникационных технологий (ИКТ).

Результаты опроса экспертов показали, что для России наиболее эффективными путями в обеспечении импортонезависимости от иностранных средств информационных технологий являются: организация возврата в страну отечественных научных кадров; открытие высокооплачиваемых рабочих мест для иностранных специалистов; активизация работы разведывательных структур для поиска и вовлечение в отечественное производство иностранных инновационных технологий; создание в Министерстве экономического развития РФ, Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций специальных структур управления обеспечением импортонезависимости от иностранных средств информационных технологий и другие (см. Схему 2).

Для определения путей разрешения указанной проблемы в контексте этической социальной инженерии Россия может использовать лучшие образцы своего исторического (ретроспективного) опыта. Во все времена наше Отечество использовало знания, умения навыки (опыт, компетенции) зарубежных специалистов.

Так умножали авторитет, славу, могущество России иностранцы: Витус Ионассен Беринг (Иван Иванович Беринг)—мореплаватель, датчанин; Альфред Бернхард Нобель—(1801—1872)—швед, инженер, изобретатель, предприниматель; Карл Густав Эмиль Маннергейм (швед, финн); Абрам Ганнибал—потомок царского дома Эфиопии (его

правнук — Александр Сергеевич Пушкин); Бурхард Кристоф фон Мюнних — немец; Питер Эдмонд де Ласси (Пётр Петрович Ласси) — нормандец из Ирландии; Сэмюэль Грейг (Самуил Карлович Грейг) — шотландец; Левин Август фон Беннигсен (Леонтий Леонтьевич Беннигсен) — представитель баронского рода Курфюршества Ганновер; Карл Филипп Готтлиб фон Клаузевиц — немецкий военный теоретик, автор книги «О войне», император Александр I пожаловал Клаузевицу орден Святого Георгия 4-й степени и наградил его золотым оружием «За храбрость»; Луи Наполеон Жозеф Жером Бонапарт — внук младшего брата Жерома Бонапарта; Князь Петр Иванович Багратион — соратник Суворова и Кутузова, прямой потомок одного из грузинских царей. На русскую службу в юности пытался поступить и Наполеон Бонапарт.

Схема 2. Мнение экспертов об основных путях обеспечения импортонезависимости от иностранных средств информационных технологий

Этика (мораль) социальной инженерии во вражеском окружении должна объясняться тезисом: «нравственно все, что обеспечивает безопасность жизни нашего населения». В настоящее время западный мир проявил свою истинную сущность, стал жить по «правилам, а не по законам». Нарушаются, отменяются все прежде заключенные договоры, блокируются экономические отношения, вводятся экономические огра-

ничения (санкции), уничтожаются международные коммуникации. В этих условиях соблюдать, например, нормы международного патентного права, принципы этики договорных обязательств — глупо, непатриотично. В советский период, когда западные страны установили блокаду нашей стране, руководители-патриоты правильно понимали этику социальной инженерии и использовали ее для блага Отечества, не боялись использовать западные образцы техники, приборов, технологий.

Так, в 1927/28 годах на базе автомобиля Форд выпускался советский АМО-2; в 1932 года построенный американскими инженерами в Нижнем Новгороде завод ГАЗ начал выпуск копий Ford Model A. В 1967 году в Тольятти итальянцами был создан автомобильный завод — ВАЗ; «Запорожец» был скопирован с NSU Prinz 4, с International KR11 скопирован ЗиС-150; с Studebaker US6 ГАЗ 63; Танк победы Т-34 выпускался с подвеской танка Кристи, с дизельным двигателем В-2, созданным на основе австрийского двигателя фирмы «Майбах» и американского тракторного мотора; подвеска советского трактора СТЗ-5 была сделана на основе американского танка «Шерман» М4А3Е8»; на базе немецких подводных лодок была построена подлодка проекта 613; советская баллистическая ракета Р-1 — была точным клоном немецкой Фау-2.

Этически эффективно работала и наша разведка методами социальной инженерии. Советскими спецслужбам была завербована группа инженеров-ракетчиков Г. Греттрупа из команды Вернера фон Брауна, которая работала в СССР в НИИ-88 до ноября 1953 года. Считается, что советский «Буран» (1988 год) был похож на американский Шаттл. Это заслуга специалистов КГБ СССР. Заимствованы были и авиационные двигатели, а основной советский военно-транспортный самолет Ли-2, был лицензионной копией американского Douglas DC-3.

В советское время западные ученые (Кембриджская пятерка) оказали содействие в разработке ядерных технологий СССР. Считается, что в США были «заимствованы» самолет Туполева для доставки ядерной бомбы, фотоаппарат ФЭД, у Германии — фотоаппарата «Зенит-4»; телевизор Ленинград-2 — клон немецкого EFu T-1; телевизоры КВН-49 и Старт-3 — копии американского RCA 621TS и британского GEC BT2253 и другое. Заимствования были и в сфере средств информационных технологий: ЭВМ; «Система Мини-ЭВМ»; «Агат» — плагиат Apple II и другие.

Сырьевой же потенциал России для производства средств ИКТ неограничен. Так в 2023 г. наша страна Россия будет производить до 25% мирового объема высокочистого неона, который необходим для производства микросхем, чипов; из 7 млн тонн мировой ежегодной добычи высококачественного кремния, 600 000 тонн добывает Россия [7]. Апри-

ори, в современных условиях неопределенности, кризиса в странах Запада, задачи России:

а) вернуть из-за границы своих специалистов ИТК-сферы;

б) организовать исследования и конструирование инновационных средств ИТК;

в) заимствовать лучшие средства производства у западных стран.

Очевидно, что России нужны эффективные инновационные (качественные) средства ИТК, чтобы успешно организовывать информационное противоборство в ведущейся в настоящее время гибридной войне, в военном конфликте на Украине и в прогнозируемой войне с НАТО.

Эффективность обеспечения импортонезависимости средств ИТК

По уровню эффективности обеспечения импортонезависимости средств ИТК можно объяснять цену достижения цели. Категория «эффективность» в обеспечении импортонезависимости может частично быть синонимом понятий: качество, результативность, оптимальность, прилежность, полезность, экономичность. Качество—это свойство «вещи». Нет качества—нет «вещи». Нет качества—нет эффективности деятельности. Бесполезные вещи, труд не могут считаться эффективными, если организаторы производства не работают на врага с задачей развалить наше производство. Следовательно, эффективная деятельность по обеспечению импортонезависимости—качественная, полезная, экономичная, результативная деятельность. «Нечто есть благодаря своему качеству то, что оно есть, и, теряя свое качество, оно перестает быть тем, что оно есть» [3]. Некачественная деятельность структуры любой системы обусловливает либо ее ликвидацию, либо совершенствование. Очевидно, что существуют не качества, а только вещи, обладающие бесконечно многими качествами». Эффективность—отношение результата деятельности к затраченным ресурсам (материальным, моральным, политическим, временным и иным).

Высокого уровня результативности в системе обеспечения отечественной импортонезависимости от иностранных средств информационных технологий трудно достичь без целенаправленной этической подготовки кадров социальной инженерии, задачами которой являются системное нравственное воспитание, конструирование новых трудовых, правовых, нравственных отношений, традиций в научной, трудовой деятельности.

Опрос экспертов показывает, что в воздействиях на личность (коллектив, организацию, общество) социальная инженерия в контексте данного предмета выполняет следующие наиболее значимые функции

(ранговые показатели): идеологическую (формирование нравственных стереотипов поведения, создания системы ценностных и социальных предпочтений); гуманистическую (упрощает взаимодействия и взаимоотношения людей, совершенствует общественные отношения); воспитательную (регулирует нормативный порядок в обществе; служит примером для подражания; является примером организации традиционных действий людей; тренирует волю, формирует привычки сознательного подчинения традициям, нормам, правилам взаимоотношений людей); общественного контроля (создает традиционный моральный портрет личности или организации, который регулирует деловые и властные отношения; регулирует поведение людей и общностей в различных ситуациях на основе норм морали (см. Схема 3).

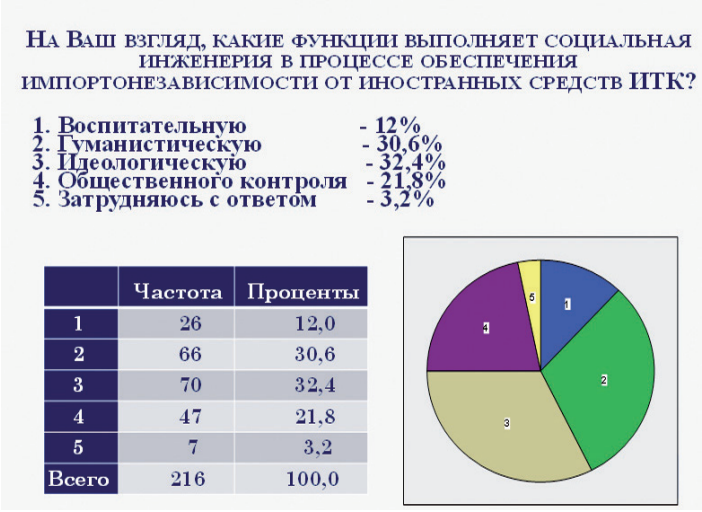

Схема 3. Мнение экспертов о функциях социальной инженерии в процессе обеспечения импортонезависимости от иностранных средств информационных технологий

Кроме этих функций определенную долю в ранговой шкале занимают:

- **познавательная** (обеспечивает прирост нового знания об отношениях в организациях; практическую обучающую среду оптимального взаимодействия в коллективе; знаниями показателей морали для оценки поведения и другое);
- **прикладная** (упрощает, формализует взаимоотношения в организации; дает конкретную информацию для разработки и принятия

управленческого решения о развитии организаций; осуществляет профилактику социального напряжения, социальных кризисов, катаклизмов, конфликтов; формирует личностные и групповые нормы социального поведения и другие);
- **прогностическая** (способствует разработке научно-обоснованных прогнозов о тенденциях развития взаимоотношений в организации); проектирования, программирования, планирования (способствует формализации, точности, прилежности в работе органов управления при реализации управленческих решений);
- **властная** (регламентирует методы и приемы подчинения начальнику, работодателю и т.п.).

В конечном итоге эффективность этической социальной инженерии в системе обеспечения отечественной импортонезависимости от иностранных средств информационных технологий в той или иной мере могут быть определены в соответствии с основным законом общественного управления, правильное выполнение которого обусловливает создание системы федеральных органов исполнительной власти. Чем лучше эта система удовлетворяет соответствующие потребности населения, тем выше она оцениваются людьми, тем качественнее работают управленцы, реализующие методы и средства этики социальной инженерии. Результаты анализа научных трудов, наблюдений практики показывают, что прямо или косвенно показателями эффективности этики социальной инженерии можно считать:

- активность населения на выборах власти, участие в разработке институтов гражданского общества;
- социально-экономическое благополучие населения; миграция (эмиграция) населения;
- стиль государственного управления; производительность труда; конфликтность в обществе;
- правовой порядок; количество протестных мероприятий (иски в суд, жалобы, митинги, демонстрации ...);
- уровень коррупции;
- патриотизм населения;
- следование позитивным традициям;
- преобладающие общественное настроение;
- коллективное мнение о власти, государстве;
- количество населения, ведущего здоровый образ жизни;
- количество инвалидов;
- средний возраст населения;
- открытость власти и многие другие.

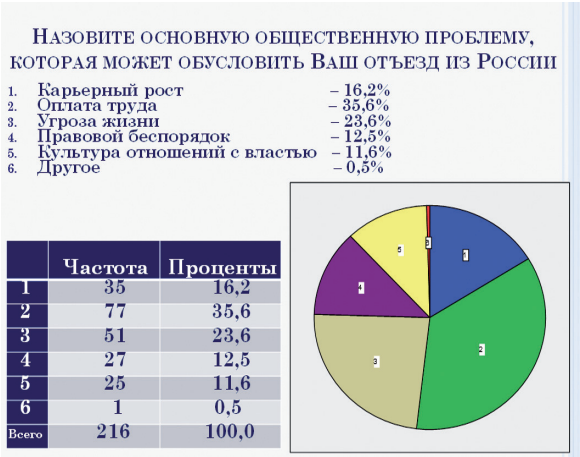

Схема 4. Мнение респондентов о причинах отъезда из страны граждан России

Априори, что люди не будут эмигрировать в западные страны, если они в России найдут высоко оплачиваемую работу, почувствуют безопасность своей семьи, ощутят работу «социальных лифтов», почувствуют уважение власти, испытают позитивные примеры удовлетворения других жизненных потребности (см. Схему 4).

Заключение

Таким образом, импортонезависимость экономики—одна из основ обеспечения национальной безопасности России в условиях ведения против нее гибридной войны. Особую важность приобретает независимость от средств информационных цифровых технологий, т.к. они обеспечивают все общественные коммуникации. Этическая социальная инженерия регламентирует деятельность в системе обеспечения импортонезависимости на высоком уровне качества, прилежности, нравственности, эффективности, производительности, инициативы, организованности.

Отдельные элементы системы этической социальной инженерии в системе обеспечения отечественной импортонезависимости от иностранных средств информационных технологий представлены в трудах российских ученых, но их содержание пока остается мало востребованными российской практикой. В части сообщества специалистов ИКТ

сохраняются пессимистические настроения, неуверенность в перспективах решения рассматриваемой проблемы, что, вероятно, обусловлено ограниченным знанием дореволюционного российского и советского опыта.

Наиболее эффективными путями в обеспечении импортонезависимости от иностранных средств информационных технологий являются: организация возврата в страну отечественных научных кадров; открытие высокооплачиваемых рабочих мест для иностранных специалистов; активизация работы разведывательных структур для поиска и вовлечение в отечественное производство иностранных инновационных технологий; создание в Министерстве экономического развития РФ, Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций специальных структур управления обеспечением импортонезависимости от иностранных средств информационных технологий и другие.

Эффективная деятельность по обеспечению импортонезависимости — качественная, полезная, экономичная, результативная деятельность. Социальная инженерия в контексте данного предмета выполняет несколько значимых функций: идеологическую, гуманистическую, воспитательную, общественного контроля. Показателями эффективности этики социальной инженерии могут быть качество реализации основных потребностей населения, которые сопряжены с количеством федеральных органов исполнительной власти.

Список источников

1. Абакумов С. А. Развитие гражданского общества как фактор оптимизации социального контроля над деятельностью государства в условиях глобализации: Социологический аспект. Автореферат дис. ... кандидата социологических наук : 22.00.08 / Соврем. гуманит. акад. — Москва, 2006. – 24 с.

2. Вышегородцев В. В. Вместо импортозамещения — импортонезависимость // Интерфакс, 30 Июня 2022 г. [Электронный ресурс] URL: https://www.interfax.ru/russia/849654 (дата обращения 06.06.2023).

3. Гегель Г. В. Ф. Энциклопедия философских наук. Часть первая. Логика. — Соч. — Т. 1. — М.: Госиздат, 1929. — С. 157.

4. Гостев А. Н. Международное цифровое доверие в социально-экономической сфере: социолого-управленческой представление // Вестник Академии права и управления. — 2022. — № 1(66). — С. 80-88.

5. Ламинина О. Г. Возможности социальной инженерии в информационных технологиях // Гуманитарные, социально-экономические и общественные науки.—2017. –№2.– С. 5-11.

6. АРПП «Отечественный софт». Российское ПО для импортозамещения. 2009-2022 [Электронный ресурс] URL: https://arppsoft.ru/catalog (дата обращения 06.06.2023).

7. Список стран по производству кремния. 17 ноября 2022 г. [Электронный ресурс] URL: https://www.statista.com/statistics/268108/world-silicon-production-by-country (дата обращения 06.06.2023).

8. Тепляков С. П., Тимохович А. С. Социальная инженерия. Анализ и методы защиты // Academy.—2018.—№ 7 (34) .—С. 26-27.

Об авторе

Гостев Александр Николаевич—
доктор социологических наук, профессор, профессор кафедры информационной культуры цифровой трансформации, Московский государственный лингвистический университет (Россия, Москва).
E-mail: Gostevan@inbox.ru.

About the author

Alexander N. Gostev—
Doctor of Sociological Sciences, Professor, Professor of the Department of Information Culture of Digital Transformation, Moscow State Linguistic University (Russia, Moscow).
E-mail: Gostevan@inbox.ru.

УДК 004.056

ИНСТРУМЕНТЫ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ КАК УГРОЗА КОНФИДЕНЦИАЛЬНЫМ ДАННЫМ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Пискунова В. В.
Московский государственный лингвистический университет (Россия, Москва).
piskunova.nika@mail.ru

Научный руководитель:
Елин В. М.
Московский государственный лингвистический университет (Россия, Москва).
elin_vm@mail.ru

Аннотация

Статья раскрывает особенности применения инструментов социальной инженерии как угрозы получения несанкционированного доступа и (или) утечки конфиденциальных данных. В статье рассматривается нормативная документация Российской Федерации на настоящий момент по рассматриваемым вопросам. Выделены положительные результаты применения указанных технологий и сформулированы предложения о необходимости совершенствования действующего законодательства.

Ключевые слова

Социальная инженерия, конфиденциальная информация, угрозы, меры противодействия.

Для цитирования: Пискунова В. В. Инструменты социальной инженерии как угроза конфиденциальным данным в российской федерации // Hi-Hume Journal.—2023.—№ 1 (1).—С. 61—68.

TOOLS OF SOCIAL ENGINEERING AS A THREAT CONFIDENTIAL DATA IN THE RUSSIAN FEDERATION

Veronika V. Piskunova
Moscow State Linguistic University (Moscow, Russia).
piskunova.nika@mail.ru

Scientific supervisor
Vladimir M. Elin
Moscow State Linguistic University (Moscow, Russia).
elin_vm@mail.ru

Abstract
The article touches upon the features of social engineering tools as a threat of unauthorized access and (or) leakage of confidential data. The paper considers the regulatory documentation of the Russian Federation on the issues under consideration. The positive results of current regulation are highlighted and proposals on the need to improve legislation are formulated.

Keywords
Social engineering, confidential information, threats, counteraction measures.

For citation: Piskunova V. V. Tools of social engineering as a threat to confidential data in the Russian Federation // Hi-Hume Journal.—2023.—№ 1 (1).—Pp. 61—68.

В настоящее время в Российской Федерации делается сильный акцент на развитии информационных технологий и внедрении цифровой трансформации и информатизации во все сферы жизни общества и бизнес-процессы, включая критические. Однако наряду с этими достижениями растет озабоченность по поводу контроля и регулирования влияния цифровой среды на страну и ее граждан. Это связано с возникающими рисками в цифровой сфере и необходимостью их эффективного устранения.

Для решения этих проблем необходимо выявить и перестроить слабые и уязвимые стороны в широкомасштабной цифровизации, в том числе вузовской подготовки специалистов по информационной безопасности [8]. Это включает в себя совершенствование правовой базы, регулирующей данную область, и разработку государственной политики, способствующей ее безопасной и надежной реализации.

Одной из обратных сторон технического прогресса является одновременный и параллельный рост возможностей киберпреступников. Они постоянно совершенствуют свои методы и приемы совершения киберпреступлений, тем самым расширяя спектр вероятных угроз. Важно

признать, что угрозы информационной безопасности выходят за рамки технических аспектов [7] и охватывают и другие области.

В сфере информационной безопасности социальная инженерия — это практика, оперирующая различными методами для получения конфиденциальной или личной информации. Она включает в себя понимание человеческой психологии и поведения, особенно в тех случаях, когда люди действуют и реагируют в нестандартных и стрессовых ситуациях. Путем манипулирования людей принуждают к разглашению конфиденциальных данных или выполнению определенных действий и процедур.

В целом, по мере перехода России к цифровой трансформации крайне важно решать возникающие проблемы и риски, связанные с информационной безопасностью. Для этого требуется комплексный подход, сочетающий технические меры, правовые аспекты и государственную политику для обеспечения безопасного и надежного использования цифровых технологий.

Федеральная служба по техническому и экспортному контролю (ФСТЭК) придает все большее значение проблеме социальной инженерии, так как это потенциальная возможность получения несанкционированного доступа к системе или получения данных конфиденциального характера. В связи с чем включает в банк угроз такие угрозы как УБИ.173 Угроза «спама» веб-сервера, УБИ.174 Угроза «фарминга», УБИ.175 Угроза «фишинга» [1]. Исходя из этого, социальная инженерия представляет особую опасность информационной безопасности (в том числе и на государственном уровне), поскольку она опирается на человеческие ошибки, а не на слабые места и протоколы в программном обеспечении и операционных системах.

При этом следует иметь в виду, что к конфиденциальным данным относятся различные виды информации [4]. Сюда входят персональные данные, состоящие из фактов, событий и изменений в личной жизни человека. Включается также информация, относящаяся к текущим расследованиям в рамках уголовно-процессуального кодекса и судебным разбирательствам, известная как тайна следствия и судопроизводства. К государственной тайне относится служебная информация, доступная только ограниченным органам государственной власти, как это определено Гражданским кодексом Российской Федерации и федеральными законами. Кроме того, в перечень конфиденциальной информации включается информация, связанная с профессиональной деятельностью (медицинская, нотариальная, адвокатская тайны), а также обеспечивается ограниченный доступ к переписке, телефонным разговорам, почте, телеграфным сообщениям и другим формам связи. Информация,

относящаяся к коммерческой деятельности, доступ к которой ограничен Гражданским кодексом Российской Федерации и федеральными законами, составляет коммерческую тайну. При этом сведения об изобретениях, полезных моделях или промышленных образцах до их официального опубликования также считаются конфиденциальными. Наконец, в эту сферу попадают сведения, содержащиеся в делах об отдельных нарушениях, и сведения об уголовной ответственности в делах с участием органов власти и должностных лиц.

Социальная инженерия играет одну из ключевых ролей в совершении мошенничества в сфере компьютерной информации [3]. В соответствии с Уголовным Кодексом Российской Федерации под мошенничеством в сфере компьютерной информации понимаются действия, связанные с хищением чужого имущества либо с приобретением права на чужое имущество путем извлечения, блокирования, модификации, удаления и иных манипуляций с цифровой информацией; средствами хранения, обработки или передачи данных; информационно-телекоммуникационными сетями.

Так, по заявлению Генпрокуратуры, в 2020 году количество преступлений с использованием информационно-коммуникационных технологий в России увеличилось в 11 раз за 5 лет. Общее число киберпреступлений, зарегистрированных в 2020 году, составляет более 510,4 тысяч, из которых 70% являются кибермошенничествами. Таких инцидентов на 73,4% больше по сравнению с 2019 годом. В 2021 году в России было зафиксировано около 518 000 киберпреступлений, что на 1,4% больше, чем в предыдущем году, в частности, количество жалоб на мошенничество (хищение ценностей с целенаправленным введением в заблуждение потерпевшего) увеличилось на 5,1%, превысив отметку в 249 000. Статистика составлена на основе данных от ООО Группа компаний «РТМ», которое провело оценку на основании возбужденных уголовных дел, связанных с применением информационных технологий [13].

Тактика социальных инженеров строится на обмане доверия, попытках ввести жертву в заблуждение, выводя ее из стабильного эмоционального состояния. Цель—привести человека в состояние аффекта, в результате чего он мыслит нерационально и совершает нелогичные поступки. Инструменты социальной инженерии широко распространены благодаря общедоступности, убедительности и эффективности. Исходя из этого, именно методы противодействия социальной инженерии могут нейтрализовать большинство угроз информационной безопасности, так как данные приемы предотвращают переход авторизованного пользователя в статус внутреннего нарушителя безопасности [12].

Ошибки пользователей гораздо менее предсказуемы, что затрудняет их выявление и предупреждение, нежели вторжение в систему на основе вредоносных программ.

Разработка нормативных документов, стратегий и мер по борьбе с инструментами социальной инженерии на законодательном уровне в Российской Федерации в настоящее время представляется недостаточной, так как не охватывает всего разнообразия, а представляет только ее узкий аспект. Различные источники литературы [9, 10, 11] подчеркивают широкий спектр методов и инструментов, используемых в практиках социальной инженерии. Эти методы включают в себя:

- предлог — искусственно смоделированный сценарий для получения информации;
- дорожное яблоко — съемный носитель информации с вредоносным программным обеспечением, оставленный в людном месте или переданный непосредственной жертве;
- quiproquo — обмен фальшивого актива на реальный;
- следование за легитимным пользователем или посетителем в контролируемую зону;
- фишинг — рассылка поддельных сообщений с целью получения информации, чаще всего встречается в форме массовых и рассредоточенных рассылок;
- целевой фишинг — фишинг, сфабрикованный для конкретных получателей сообщения на основе предварительно проведенной информационной разведки (OSINT) или утекших данных;
- вишинг — форма фишинга по телефону;
- смишинг — разновидность фишинга через SMS-сообщения;
- фаззинг — сообщение или обращение с чрезмерным количеством деталей, которые перегружают контекст, но дают убедительное описание;
- дезориентация и ввод в заблуждение;
- спекуляции;
- плечевой серфинг — считывание данных с активного дисплея жертвы;
- honeypot — ресурс, выполняющий задачи привлечения и вовлечения;
- фейковые новости и фейковые отзывы, направленные на создание интриги, влияния на общественное мнение [14, с. 63–103].

Приведенный перечень не является исчерпывающим и может быть дополнен. Показательно, что при проведении атак задействуются сразу несколько социоинженерных тактик, при этом ни в зарубежном, ни в

российском законодательстве получение доступа, перехват или утечка конфиденциальных данных не рассматриваются как отдельные угрозы, а учитываются как один из этапов вектора атаки или используемая тактика / техника в сценарии реализации угрозы. Так, например, в методике MITRE ATT&CK [10] инструменты социальной инженерии представлены как техники разведки, способы получения первоначально доступа, приемы бокового движения (методы, которые злоумышленники используют для входа и управления удаленными системами в сети), перехвата. В Методике оценки угроз безопасности информации ФСТЭК [6, с. 65–83] они представлены как техники сбора информации о системах и сетях, техники получения первоначального доступа к компонентам систем и сетей.

Следует также обратить внимание на подход, представляемый нормами технического регулирования. Так, стандартами [2] и методикой [6] предлагаются технологические инструменты оценки и противодействия угрозам информационной безопасности. Рассмотренные меры представляются недостаточными, поскольку приведенная ранее статистика демонстрирует увеличение количества инцидентов, связанных с применением информационных технологий, особенно по части кибермошенничеств.

В перспективе следует разработать методические рекомендации противодействия социальной инженерии в области защиты конфиденциальной информации, в том числе — персональных данных. Для предотвращения возникновения утечки информации и иных инцидентов информационной безопасности компании и организации должны разработать внутренние документы согласно последним требованиям законодательства [5]. Более того, комплекс организационно-методических мероприятий, направленных на минимизацию риска от реализации социоинженерной угрозы, должен учитывать обучение граждан для предотвращения раскрытия своих личных данных.

Список источников

1. Банк данных угроз безопасности информации. Официальный сайт ФСТЭК России [Электронный ресурс] URL: https://bdu.fstec.ru/ (дата обращения: 17.11.2022).

2. ГОСТ Р ИСО/МЭК ТО 18044—2007. Информационная технология — Методы и средства обеспечения безопасности — Менеджмент инцидентов информационной безопасности [Электронный ресурс] URL: https://docs.cntd.ru/document/1200068822 (дата обращения: 17.11.2022).

3. Уголовный Кодекс РФ Статья 159.6. Мошенничество в сфере компьютерной информации // «Уголовный кодекс Российской Федерации» от 13.06.1996 N 63-ФЗ (ред. от 24.09.2022) [Электронный ресурс] URL: http://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения: 17.11.2022).

4. Указ Президента Российской Федерации от 06.03.1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера». Официальный сайт Администрации Президента России [Электронный ресурс] URL: http://www.kremlin.ru/ (дата обращения: 17.11.2022).

5. Указ Президента Российской Федерации от 01.05.2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации». Официальный сайт Администрации Президента России. [Электронный ресурс] URL: http://www.kremlin.ru/ (дата обращения: 17.11.2022).

6. Методический документ: Методика оценки угроз безопасности информации. Официальный сайт ФСТЭК России. [Электронный ресурс] URL: https://bdu.fstec.ru/ (дата обращения: 17.11.2022).

7. Бирин Д. А., Мельников С. Ю., Пересыпкин В. А. Об эффективности средств коррекции искаженных текстов для результатов работы систем распознавания / В сборнике: Суперкомпьютерные технологии (СКТ-2018). Материалы 5-й Всероссийской научно-технической конференции.—Ростов-на-Дону: Южный федеральный университет, 2018.—С. 71-75.

8. Былевский П. Г. Некоторые особенности интеграции инновационных технологий и методик в высшее гуманитарное образование / Инновационные технологии обучения в вузах. Сборник статей национальной научно-практической конференции.—Сочи—Москва: ОЧУ ВО «Московский инновационный университет», 2022.—С. 40-45.

9. Число киберпреступлений в России. TAdviser [Электронный ресурс] URL: https://www.tadviser.ru (дата обращения: 17.11.2022).

10. ATT&CK Matrix for Enterprise. Официальныйсайт MITRE ATT&CK. [Электронный ресурс] URL: https://attack.mitre.org/ (дата обращения: 17.11.2022).

11. Evans L. Cybersecurity. An Essential Guide to Computer and Cyber Security for Beginners, Including Ethical Hacking, Risk Assessment, Social Engineering, Attack and Defense Strategies, and Cyberwarfare.—Independently published, 2018.—116 p.

12. Hadnagy C. Social Engineering: The Science of Human Hacking Paperback. Second Edition.—Hoboken: Wiley, 2018.—320 p.

13. Kiser Q. Computer Networking and Cybersecurity: A Guide to Understanding Communications Systems, Internet Connections, and Network Security Along with Protection from Hacking and Cyber Security Threats Hardcover.—Primasta, 2020.—242 p.

14. Meeuwisse R. How to Hack a Human: Cybersecurity for the Mind.—Cyber Simplicity Ltd, 2019.—230 p.

Об авторах

Пискунова Вероника Витальевна—
студент 2 курса (магистратура)
Московского государственного
лингвистического университета
(Россия, Москва);
специалист по информационной
безопасности ГК «Сател»
(Россия, Москва).
E-mail: piskunova.nika@mail.ru.

Елин Владимир Михайлович—
кандидат педагогических наук,
доцент кафедры информационной
культуры цифровой трансформации
Института информационных наук
Московского государственного
лингвистического университета
(Россия, Москва).
E-mail: elin_vm@mail.ru.

About the authors

Veronika V. Piskunova —
2nd year student (Master's degree)
Moscow State Linguistic University
(Moscow, Russia);
Information security specialist
GC «Satel» (Moscow, Russia).
E-mail: piskunova.nika@mail.ru.

Vladimir M. Elin —
Candidate of Pedagogical Sciences,
Associate Professor of the Department
of Information Culture of Digital
Transformation of the Institute
of Information Sciences of the
Moscow State Linguistic University
(Russia, Moscow).
E-mail: elin_vm@mail.ru.

УДК 004.83

ТЕХНОЛОГИИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ПРОТИВОДЕЙСТВИИ КИБЕРБУЛЛИНГУ

Мельникова А. А.
Московский государственный лингвистический университет (Россия, Москва)
pndlv12@gmail.com

Садыхбекова Л. Д.
Московский государственный лингвистический университет (Россия, Москва)
sdlyaman@yandex.ru

Научный руководитель:
Цацкина Е. П.
Московский государственный лингвистический университет (Россия, Москва)
elena-tsatskina@yandex.ru

Аннотация

Общение в виртуальном пространстве создает ощущение анонимности и безнаказанности за неэтичное, деструктивное и противоправное поведение. Переписка в социальных сетях, общение на форумах и в чатах порождает новые формы агрессивного общения, цели которого могут быть разными. Технологии искусственного интеллекта могут стать ключевыми в комплексе мер по противодействию кибербуллингу.

Ключевые слова

Борьба с кибербуллингом, машинное обучение, социальные сети, цифровые платформы для коммуникации

Для цитирования: Мельникова А. А., Садыхбекова Л. Д. Технологии искусственного интеллекта в противодействии кибербуллингу // Hi-Hume Journal.—2023.—№ 1 (1).—С. 69—76.

ARTIFICIAL INTELLIGENCE TECHNOLOGIES IN COUNTERING CYBERBULLYING

Alina A. Melnikova
Moscow State Linguistic University (Moscow, Russia)
pndlv12@gmail.com

Liaman D. Sadykhbekova
Moscow State Linguistic University (Moscow, Russia)
sdlyaman@yandex.ru

Scientific supervisor
Elena P. Tsatskina
Moscow State Linguistic University (Moscow, Russia)
elena-tsatskina@yandex.ru

Abstract
Communication in the virtual space creates a sense of anonymity and impunity for unethical, destructive and illegal behavior. Correspondence in social networks, communication on forums and in chat rooms generates new forms of aggressive communication, the goals of which may be different. Artificial intelligence technologies can become key in the complex of measures to counter cyberbullying.

Keywords
The fight against cyberbullying, machine learning, social networks, digital platforms for communication.

For citation: Melnikova A. A., Sadyhbekova L. D. Artificial intelligence technologies in countering cyberbullying // Hi-Hume Journal.—2023.—№ 1 (1).—Pp. 69—76.

Одной из важных составляющих взаимоотношений людей является общение. В современном мире распространенность информационных технологий и доступность Интернета привели к появлению новой формы травли, так называемого кибербуллинга. Кибербуллинг представляет травлю, происходящую с помощью использования технологий и Интернета. Особое распространение кибербуллинг получил среди подростков и молодых людей. В отличие от традиционных форм травли, он обладает рядом особых свойств:

- анонимность, которую предоставляют многие сайты;
- дистанционность, проявляющаяся в том, что обидчик совершает запугивание через технологии на расстоянии;
- большое количество свидетелей и бесконтрольное распространение информации, которые предоставляет Интернет.

Кибербуллинг может проходить в социальных сетях, в приложениях для обмена сообщениями, по электронной почте, на игровых платформах и мобильных телефонах. Это повторяющиеся эпизоды, цель которых — напугать, разозлить или опозорить тех, кого преследуют. Кибербуллинг может представлять собой:

- распространение ложной информации;
- шантаж или размещение компрометирующих фотографий кого-либо в социальных сетях;
- отправку оскорбляющих сообщений или угроз через платформы обмена сообщениями;
- выдачу себя за другое лицо и отправка непристойных сообщений от его имени
- и другие (Схема 1).

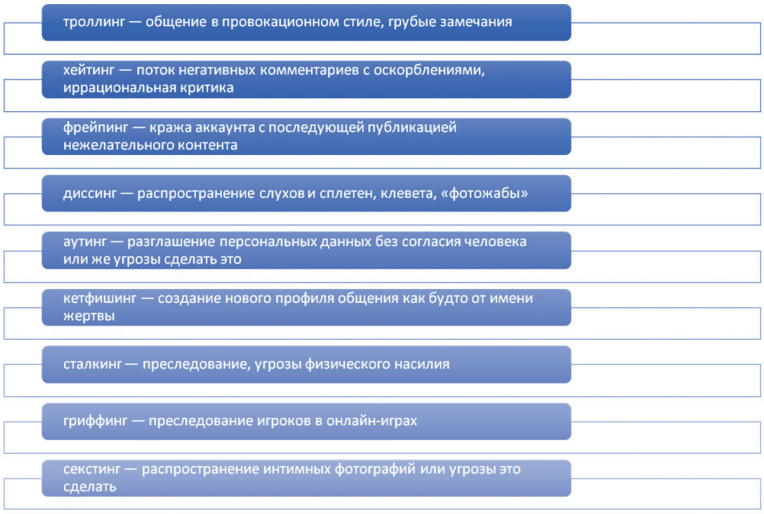

Схема 1. Формы агрессии

Такой вид действий в сети является достаточно распространенным явлением. Согласно исследованиям [3], 58% российских интернет-пользователей сталкивались с онлайн-агрессией. Каждый четвертый был мишенью такого поведения, и только 4% опрошенных признаются, что были инициаторами травли. Действия кибербуллинга могут иметь долгосрочные психологические, эмоциональные и физиологические последствия для человека, который стал жертвой Интернет-травли. К со-

жалению, на данный момент нет достаточного количества инструментов для борьбы с травлей.

В России проблема кибербуллинга уже несколько лет обсуждается на высшем уровне. В декабре 2021 года на встрече с членами Совета по развитию гражданского общества и правам человека (СПЧ) президент России Владимир Путин поднял проблему буллинга и обозначил необходимость ввести практику обсуждения вопросов по этой теме.

Тем не менее, на сегодняшний день специального закона против кибербуллинга в России не существует. Однако пользователи, столкнувшиеся с травлей в сети, могут обратиться к администраторам социальной сети или сайта с просьбой удалить недостоверные сведения. В случае систематического бездействия последних—в правоохранительные органы, где заявление рассмотрят на предмет попадания под ряд статей УК РФ. Например, оскорбление религиозных чувств верующих—статья 148 УК РФ, доведение до самоубийства—статья 110 УК РФ, угрозы—статья 119 УК РФ, клевета—128.1 УК РФ, шантаж и вымогательство—163 УК РФ. Однако, необходимы нормы, которые относились бы непосредственно к Интернет-пространству.

Государство стремится привлечь к ответственности не только самих зачинщиков травли, но и социальные сети. Прямое, адресное проявление агрессии может веерно касаться всех пользователей и провоцировать массовою травлю, являться средством манипулирования сознанием, выражаться в провокациях на совершение неэтичных и противоправных действий выходящих за пределы цифровых платформ. С 1 февраля 2021 года в России действует закон о самоконтроле социальных сетей. Он обязывает онлайн-площадки самостоятельно выявлять и удалять сообщения, содержащие противоправный контент в том числе: экстремизм, призывы к насилию и терроризму, порнографию, информацию об изготовлении и использовании наркотиков, совершении самоубийства и прочее.

Исследование проблемы агрессивной коммуникации имеет многосторонний характер и изучается в этических, правовых, психологических и лингвистических аспектах. Формы проявления агрессии развиваются и совершенствуются, в связи с этим поиск путей противостояния кибербуллингу должен пополняться современным инструментарием. Одним из направлений в искусственном интеллекте, открывающим множество возможностей для предотвращения кибербуллинга, является интеллектуальный анализ текстов, основанный на машинном обучение. В настоящее время существует множество инициатив по созданию и обучению алгоритмов, способных обнаруживать ненавистнические и

оскорбительные высказывания в Интернете, чтобы не дать пользователю увидеть их и, следовательно, подвергнуться кибербуллингу.

Преимущество таких алгоритмов перед программами родительского контроля и блокировщиками ключевых слов заключается в том, что они должны распознавать тонкие и саркастические комментарии — задача, с которой прежние решения не справляются. Кроме того, использование машинного обучения необходимо, поскольку оскорбления часто могут быть, намеренно или нет, написаны с ошибками.

Существует алгоритм автоматического обнаружения издевательств в текстах социальных сетей. В своем экспериментальном состоянии он значительно преуспел в распознавании оскорбительного поведения в Интернете на английском и голландском языках. Ученые, стоящие за этим проектом, называют тот факт, что их система может обнаруживать сигналы издевательств, своим главным достижением [4].

Этот алгоритм также определяет, кто является хулиганом, жертвой и сторонними наблюдателями в каждой ситуации, что может помочь модератору веб-сайта выполнять свою работу быстрее и эффективнее.

Другое исследование привлекает более пристальное внимание к ограничениям фильтрации по ключевым словам. Основываясь на данных, собранных на платформе Reddit, исследователи пришли к выводу, что многие актуальные слова используются как группами ненависти, так и группами поддержки, что затрудняет фильтрацию определения того, что есть что. Вместо этого в данном исследовании. предлагается обучить алгоритм распознаванию данных, создаваемых сообществами, которые «соответствуют языковой идентичности» групп ненависти. При этом он сможет видеть шаблоны, типичные для таких групп и сообществ, в постах в социальных сетях и других интернет-ресурсах [4].

Кроме того, на платформе Instagram была запущена функция, направленная на борьбу с кибербуллингом. Данная функция работает на основе алгоритмов искусственного интеллекта. Она уведомляет людей, когда подписи к их фото или видео могут считаться оскорбительными. Пользователям дается возможность отредактировать написанное, однако это не обязательно. Но даже если пользователь опубликует комментарий или пост и после более глубокого анализа выяснится, что он содержит оскорбительные высказывания, другие пользователи платформы его просто не увидят.

Алгоритмы машинного обучения уже могут с высокой точностью выявлять суицидальные наклонности на основе нейронного представления эмоций. В будущем эмоциональный искусственный интеллект может стать бесценным помощником в распознавании и предотвращении

членовредительства. Если машина способна понимать человеческие эмоции на основе распознавания голоса или лица, это будет означать огромный скачок вперед для использования искусственного интеллекта в предотвращении самоубийств.

Несмотря на то, что их ранние стадии были довольно успешными, алгоритмам искусственного интеллекта по борьбе с ненавистническими высказываниями еще предстоит пройти долгий путь. Вероятно, самая большая проблема для машинного обучения заключается в том, насколько трудно определить, что является разжиганием ненависти, а что нет. Например, одно и то же предложение может признаваться и ненавистным, и допустимым. Все зависит от культурного и социального уровней, а так же гражданства и национального происхождения автора.

Кроме того, отсутствует однозначное определение «разжигания ненависти». В статье 282 Уголовном кодексе РФ, описываются действия, направленные на возбуждение ненависти либо вражды, а также на унижение достоинства человека. Цифровые коммуникационные платформы объединяют в общении представителей разных поколений, стран, культур, конфессий, социальных слоев и др. Стремительное развитие сквозных технологий и их внедрение во все сферы жизни и деятельности людей влекут собой неизбежность цифровых трансформаций, устоявшихся культурных, социальных, экономических и финансовых процессов, что в свою очередь является толчком для развития и совершенствования имеющихся технологий [2]. Таким образом возникает зависимость, которую можно выразить круговым графом.

Схема 2. Цифровые трансформации социокультурных и производственных процессов, сопряжённые с кибербуллингом

Кибербуллинг — явление социальное, в него включены не только жертвы и агрессоры. В зависимости от формы агрессии и цели, которую преследует зачинщик, все участники выходят за рамки цифровой платформы и виртуального мира и переносят свое состояние, поведение и отношение к людям и событиям в реальную жизнь [1].

Выводы

Наряду с международными проблемами терроризма и сохранения национальной безопасности появляется вопрос расширения комплекса мер борьбы с кибербуллингом. Хотя большинство упомянутых выше решений все еще находятся на стадии эксперимента, авторами статьи они рассматриваются как многообещающие и перспективные в комплексе мер противодействию кибербуллингу. Важно понимать, что в случае эффективной их реализации кибербуллинг полностью не прекратит свое существование.

Более того, будут найдены пути обхода интегрированных в цифровые платформы алгоритмов. Возможно, человечество ожидает что-то вроде гонки вооружений между технологиями, направленными против агрессии в киберпространстве и технологиями, способствующими им. Таким образом, использование технологий искусственного интеллекта позволит частично или на какой-то период повысить эффективность комплекса мер по противодействию кибербуллингу, но полностью не искоренит его.

Список источников

1. Могунова М. М. Кибербуллинг как новая опасность / М. М. Могунова // Вестник СКУ им. М. Козыбаева. — 2021. — № 2 (51). — С. 99-106.

2. Цацкина Е. П. О возрастающей роли гуманитарной составляющей в обеспечении информационной безопасности / Е. П. Цацкина // Информационная безопасность и межкультурная коммуникация в контексте цифровой трансформации: Сборник научных трудов / Редакционная коллегия: П.Г. Былевский (отв. редактор) [и др.]. — Москва: Московский государственный лингвистический университет, Медиа Группа «Авангард», 2022. — С. 145-152.

3. Исследование: 58% интернет-пользователей сталкивались с онлайн-агрессией. «Такие Дела» 12 ноября 2019 г. [Электронный ресурс]. URL: https://takiedela.ru/news/2019/11/12/kiberulling/?ysclid=lbf8o8w4hr652723157 (дата обращения 12.05.2023).

4. Национальная библиотека медицины США.—[Электронный ресурс].—URL: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6175271/ (дата обращения 12.05.2023).

Об авторах

Мельникова Алина Александровна—
студент 4 курса (бакалавриат)
Московского государственного
лингвистического университета
(Россия, Москва).
E-mail: pndlv12@gmail.com.

Садыхбекова Ляман Джамиль кызы—
студент 4 курса (бакалавриат)
Московского государственного
лингвистического университета
(Россия, Москва).
E-mail: sdlyaman@yandex.ru.

Цацкина Елена Петровна—
кандидат педагогических наук, доцент
ВАК, доцент кафедры международной
информационной безопасности
Института информационных наук
Московского государственного
лингвистического университета
(Россия, Москва).
E-mail: elena-tsatskina@yandex.ru.

About the authors

Alina A. Melnikova—
4th year student (bachelor's degree)
Moscow State Linguistic University
(Russia, Moscow).
E-mail: pndlv12@gmail.com.

Lyaman J. Sadikhbekova—
4th year student (bachelor's degree)
Moscow State Linguistic University
(Russia, Moscow).
E-mail: sdlyaman@yandex.ru.

Elena P. Tsatskina—
Candidate of Pedagogical Sciences,
Associate Professor of the Higher
Attestation Commission, Associate
Professor of the Department
of International Information Security
of the Institute of Information
Sciences of the Moscow State
Linguistic University
(Russia, Moscow).
E-mail: elena-tsatskina@yandex.ru.

УДК 004.03

ЯЗЫКОВОЕ МОДЕЛИРОВАНИЕ УГРОЗ И СПОСОБОВ ИХ МИНИМИЗАЦИИ

Пелих Я. В.
Московский государственный лингвистический университет, Москва
pelikh031@gmail.com

Научный руководитель
Гостев А. Н.
Московский государственный лингвистический университет (Россия, Москва)
Gostevan@inbox.ru.

Аннотация
В настоящей статье утверждается, что фразообразующие модели имеют генеративный характер, что подчеркивает их способность к эвристике. Кроме того, развивается идея о многоуровневой системе фразообразующих моделей.

Ключевые слова
Нейронная сеть, искусственный интеллект, языковые модели, угрозы, информация, автоматизированные средства.

Для цитирования: Пелих Я. В. Языковое моделирование угроз и способов их минимизации // Hi-Hume Journal.—2023.—№ 1 (1).—С. 77—80.

LANGUAGE MODELING OF THREATS AND WAYS TO MINIMIZE THEM

Yaroslavna V. Pelikh,
Moscow State Linguistic University (Moscow, Russia)
pelikh031@gmail.com

Scientific supervisor
Alexander N. Gostev
Moscow State Linguistic University (Moscow, Russia)
Gostevan@inbox.ru.

Abstract

In this article, it is argued that phrase-forming models have a generative character, which emphasizes their ability to heuristics. In addition, the idea of a multilevel system of phrase-forming models is being developed.

Keywords

Neural network, artificial intelligence, language models, threats, information, automated tools.

For citation: Pelikh Ya. V. Language modeling of threats and ways to minimize them // Hi-Home Journal.—2023.—№ 1 (1).—Pp. 77—80.

Нельзя недооценивать опасность использования автоматизированных средств для создания пропагандистских сообщений [6]. Генеративная модель может использоваться для создания фальшивых данных. Нейронная сеть понятия не имеет, что такое ложь. Нейронные сети могут находить неочевидные для человека закономерности в данных, которые используются в их обучении, а затем использовать их при анализе новых данных.

Архитектура нейронной сети и качество данных, на которых она обучалась, влияют на точность анализа данных. Насколько хорошо нейронная сеть будет определять ложь, зависит от того, сколько данных было использовано для ее обучения. Это не зависит от того, выпущена та или иная модель или нет, в рамках неизбежной тенденции к удешевлению производства привлекательного цифрового контента. Такие проблемы, как смещение воспроизводства, могут возникнуть, когда модели используются без дополнительных исследований, поскольку модели становятся все более доступными [5].

Создание языковых моделей и их модификация являются дорогостоящими и доступны только ограниченному числу организаций, которые стараются сделать все возможное, чтобы уменьшить проблемность генерируемых текстов [2]. Вряд ли удастся избавиться от всех положительных и отрицательных черт языковых моделей. Этика людей, которые его используют, является самой важной вещью. Право убеждать других—основное условие демократии, но те, кто занимается искусственным интеллектом, должны сохранять чувство ответственности, поскольку их деятельность влияет на сознание людей и жизнь общества.

В настоящее время развитие генеративных языковых моделей и автоматизированных систем является одним из самых активных направле-

ний в области компьютерных технологий. Однако данный процесс сопровождается как положительными эффектами, так и возникающими угрозами. Представим вам возможные меры по смягчению угроз, связанных с развитием генеративных языковых моделей и автоматизированных систем [3].

Одна из возможных угроз—это воздействие на человеческую психику. Нейросети могут создавать контент, способный может вызвать шок и негативные эмоции, что является большой проблемой. Если такое содержимое допустимо попадает в общий доступ, то может произойти окружающий эффект. Для снижения возможности подобных инцидентов необходимо уделять большое внимание регулированию контента, создаваемого автоматизированными системами.

Следующей угрозой является ложное распознавание. Оно может привести к негативным последствиям в различных областях, например, в медицине или юриспруденции. Сложные системы, используемые в машинном обучении, требуют большого числа правильных настроек и обновлений, чтобы снизить вероятность ошибки. Существенной угрозой может быть охрана конфиденциальной информации. В крупных компаниях, занимающихся созданием генеративных языковых моделей и автоматизированных систем, требуется комплексная охрана, которая бы защищала права и сведения, используемые в работе. Можно выделить несколько этапов охраны информации, таких как кодирование, зашифрование, хранение в закрытых базах данных.

Одним из важных способов смягчения угроз является повышение квалификации специалистов. Главной задачей обучения сотрудников, работающих в области разработки генеративных языковых моделей и автоматизированных систем, является формирование навыков и убеждений по обеспечению безопасности [4]. Для этого нужно углубленное профессиональное знание в области кодирования, машинного обучения, технологии blockchain и подобных направлений. Для регулирования создания и использования цифрового контента необходимы законы и международные соглашения. Также необходимо соблюдать эти законы и обеспечивать сотрудничество между правительствами. Государственные органы и производители программного обеспечения должны соблюдать законодательство о защите персональнных данных.

В конце можно сказать, что процесс развития генеративных языковых моделей и автоматизированных систем является актуальным на сегодняшний день. Возникающие угрозы могут негативно повлиять на ее развитие. Необходимо осторожно и ответственно использовать их в различных отраслях [1]. Внедрение механизмов защиты и обеспечение

конфиденциальности данных, усиление законодательства и сотрудничество между правительствами — это необходимые шаги для сохранения безопасности в мире все более автоматизированной информационной технологии. Профессиональный подход может максимально снизить вероятность проявления таких возможных угроз.

Список источников

1. Афанасьев Д. В., Крыжановская О. А. Менеджмент инновационных проектов в сфере инфокоммуникаций // Актуальные проблемы развития хозяйствующих субъектов, территорий и систем регионального и муниципального управления: материалы XI международной научно-практической конференции / под ред. Ю. В. Вертаковой. — Курск: ЗАО «Университетская книга», 2016. — С. 22-26.
2. Бова В. В. Концептуальная модель представления знаний при построении интеллектуальных информационных систем // Известия ЮФУ. Технические науки. — 2014. — № 7 (156). — С. 100-120.
3. Венделева М. А., Вертакова Ю. В. Информационные технологии управления: учебное пособие для бакалавров по специальности «Менеджмент организации». — М.: Юрайт, 2012. — 421 с.
4. Загинайлов Ю. Н. Теория информационной безопасности и методология защиты информации: учебное пособие// Ю. Н. Загинайлов.— М.-Берлин: Дирек-Медиа, 2015,— 251 с.
5. ИКТ (рынок России) [Электронный ресурс]. — URL: http:// www.tadviser.ru/index.php/ (дата обращения 06.06.2023).
6. Петренко С. А. Модель киберугроз по аналитике инноваций DARPA // Труды СПИИРАН.— 2015.— Вып. 39.— С. 26-41.

Об авторах

Пелих Ярославна Владимировна —
студент 2 курса (магистратура) Института информационных наук Московского государственного лингвистического университета, специалист ООО «ТТ-Трэвел» (Россия, Москва).
E-mal: pelikh031@gmail.com.

Гостев Александр Николаевич —
доктор социологических наук, профессор, профессор кафедры информационной культуры цифровой трансформации, Московский государственный лингвистический университет (Россия, Москва).
E-mail: Gostevan@inbox.ru.

About the authors

Yaroslavna V. Pelikh —
2nd year student (Master's degree) Institute of Information Sciences of Moscow State Linguistic University, specialist of TT-Travel LLC (Russia, Moscow).
E-mail: pelikh031@gmail.com.

Alexander N. Gostev —
Doctor of Sociological Sciences, Professor, Professor of the Department of Information Culture of Digital Transformation, Moscow State Linguistic University (Russia, Moscow).
E-mail: Gostevan@inbox.ru.

УДК 004.056

ПОВЫШЕНИЕ УРОВНЯ ПРОФЕССИОНАЛЬНОЙ КУЛЬТУРЫ ПЕРСОНАЛА, ОБСЛУЖИВАЮЩЕГО СМАРТ-СИСТЕМЫ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ К ПЕРСОНАЛЬНЫМ ДАННЫМ СОТРУДНИКОВ ВУЗОВ

Федонин А. В.
Московский государственный лингвистический университет (Россия, Москва)
avladimir2021@yandex.ru

Научный руководитель
Гостев А. В.
Московский государственный лингвистический университет (Россия, Москва)
Gostevan@inbox.ru.

Аннотация
В данной работе рассматривается актуальный вопрос совершенствования уровня профессиональной культуры персонала, занимающегося обслуживанием смарт-системы контроля и управления доступом к персональным данным сотрудников вузов. Авторы провели анализ существующих методов и технологий, необходимых для качественного выполнения этих задач, а также выявили ключевые проблемы, возникающие в процессе работы с системой. В результате изучения данных вопросов сформулированы рекомендации по повышению уровня профессиональной культуры персонала, которые позволят увеличить эффективность работы со смарт-системой контроля и управления доступом и гарантировать безопасность персональных данных сотрудников вузов.

Ключевые слова
Профессиональная культура, СКУД, этика, смарт-система, персональные данные, ВУЗ

Для цитирования: Федонин А. В. Повышение уровня профессиональной культуры персонала, обслуживающего смарт-системы контроля и управления доступом к персональным данным сотрудников вузов // Hi-Hume Journal.—2023.—№ 1 (1).—С. 81—88.

IMPROVING THE LEVEL OF PROFESSIONAL CULTURE OF PERSONNEL SERVING SMART SYSTEMS FOR MONITORING AND MANAGING ACCESS TO PERSONAL DATA OF UNIVERSITY EMPLOYEES

Alexander V. Fedonin
Moscow State Linguistic University (Moscow, Russia)
avladimir2021@yandex.ru

Scientific supervisor
Alexander N. Gostev
Moscow State Linguistic University (Moscow, Russia)
Gostevan@inbox.ru.

Abstract

In this paper, the topical issue of improving the level of professional culture of personnel engaged in the maintenance of a smart system for monitoring and controlling access to personal data of university employees is considered. The authors analyzed the existing methods and technologies necessary for the qualitative performance of these tasks, and also identified the key problems that arise in the process of working with the system. As a result of studying these issues, recommendations have been formulated to improve the level of professional culture of staff, which will increase the efficiency of working with a smart access control and management system and guarantee the security of personal data of university employees.

Keywords

Professional culture, ACS, ethics, smart system, personal data, UNIVERSITY

For citation: Fedonin A.V. Improving the level of professional culture of personnel serving smart systems for monitoring and managing access to personal data of university employees // Hi-Hume Journal.—2023.—№ 1 (1). – Pp. 81—88.

Профессиональная культура является бесценной составляющей деятельности человека, которая позволяет ему чувствовать себя уверенно и эффективно в профессиональной сфере. Она формируется под влия-

нием профессиональных знаний и культурных традиций, и выражает общественный вклад в развитие и улучшение социальных структур [4]. Поэтому, профессиональная культура является объективным показателем интеллектуальной и социальной активности личности.

Общение среди работников оказывает влияние на их ценностные ориентации, приводя к установлению общих целей, которые могут быть достигнуты путем соответствующей модификации поведения. Качество профессиональной культуры, которая характеризует отношение индивида к работе и коллегам, зависит от культуры общения и общей культуры. Последнее является фундаментальным аспектом в создании коммуникативной и профессиональной культуры, которые объединяют в себе общую культуру и культуру взаимодействия на рабочем месте.

Субъект управления, представленный менеджерами, предоставляет объекту управления—работникам информацию о том, как их работа будет осуществляться в будущем. Эти сигналы, называемые управленческими приказами, создают управленческие отношения между субъектами управления, что является необходимым условием для обеспечения управленческого взаимодействия. Таким образом, управленческие отношения являются основой административного потенциала, поскольку обеспечивают возможность выдачи административных приказов и готовность их исполнения.

Согласно теории управления, субъект управления (в качестве руководителя) направляет объекту управления (в качестве работника) сигналы воздействия, содержащие информацию о том, как следует осуществлять функционирование объекта в будущем. Такие сигналы получили название управленческих команд. Важным условием эффективного управления является существование отношений управления между субъектами, обеспечивающих возможность выдачи управленческих команд соответствующего уровня и готовность их исполнения. Управленческие отношения являются основой административного потенциала и обеспечивают способность осуществлять управленческое взаимодействие.

В соответствии с теорией управления, объект управления является конечным адресатом манипуляций управляющего субъекта, обладающего функциями руководства. Эффективность управления предполагает наличие у управляющего субъекта механизмов, способных оказать влияние на объект управления и сформировать у него мотивацию выполнения управленческих задач. Наличие данного рычага является важнейшим фактором для совершенствования управления и определя-

ет возможность реализации управляющих мероприятий. Управленческие отношения являются необходимым компонентом административного потенциала и обеспечивают способность успешной реализации управленческих функций. Профессиональная культура, включающая этические нормы и компетентность, в сочетании с этическими установками, способствует развитию личности и профессиональному росту, а также формирует стремление к самовыражению в профессиональной и политической деятельности.

В работе отмечается, что наличие высокого уровня профессиональной культуры исключительно важно для сотрудников, которые имеют доступ к конфиденциальной информации. Кроме выполнения профессиональных обязанностей, включающих разработку стратегии защиты персональных данных, эти специалисты также должны обладать высокой профессиональной культурой. Она включает в себя умение осуществлять контроль и управление доступом к личной информации, а также строго соблюдать правила безопасности и неукоснительно следовать принципам этики и деонтологии их профессии. Все это является необходимым элементом безопасной и эффективной работы с конфиденциальной информацией.

Неясность формулировок Федерального закона от 27 июля 2006 года №152-ФЗ «О персональных данных» [2], некоторых норм утверждения порядка проведения классификации информационных систем персональных данных [1] и технических документов вызывает недопонимание при обработке персональных данных в системах контроля и управления доступом. В связи с этим возникает ряд вопросов, которые требуют уточнения и улучшения правовых норм для эффективной реализации управленческих мероприятий [7]. Расхождения в трактовке терминов порождают риски получения предписаний контролирующих органов и соответствующих штрафов.

В профессиональной деятельности могут возникать следующие вопросы:

— Что следует относить к персональным данным?

— Необходимо ли получать согласие субъекта персональных данных на обработку его персональных данных?

— Требуется ли соответствующее уведомление уполномоченного органа о проводимой обработке персональных данных в системе контроля и управления доступом?

— Какие меры должны быть предприняты при обработке персональных данных для их защиты?

Система контроля и управления доступом (СКУД) использует и обрабатывает различные идентификаторы для идентификации сотрудников и посетителей на их месте работы [3]. В качестве наиболее распространенного метода идентификации часто используется фотография субъекта для предотвращения передачи идентификатора третьим лицам. Однако, несмотря на свою эффективность при автоматическом установлении личности, использование фотографии в СКУД подразумевает обработку биометрических персональных данных. Для того, чтобы фотография могла быть отнесена к биометрическим персональным данным, необходимо ее получение соответствовало требованиям, установленным ГОСТ Р ИСО/ МЭК 19794-5-2013, с учетом таких параметров, как освещение, положение головы, разрешение изображения и других нормативных требований.

В соответствии с требованиями закона биометрические персональные данные, которые используются оператором для установления личности субъекта персональных данных, могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных. Что и требует регулятор от оператора персональных данных, которым является собственник СКУД.

В рамках функционирования системы контроля и управления доступом в сочетании с другими механизмами обеспечивается комплексная защита объектов от террористических угроз, что является соответствующим требованиям законодательных актов, включая ст. 11, п. 2, который предусматривает возможность обработки биометрических персональных данных без согласия субъекта в случаях, определенных законодательством Российской Федерации, в том числе относящимися к обороне, безопасности и противодействию терроризму. При наличии достаточно крупного объекта, обеспечивающего антитеррористическую защиту в соответствии с утвержденным и согласованным паспортом, система контроля и управления доступом является одной из прописанных мер защиты.

Кроме того, оператор вправе осуществлять обработку персональных данных без уведомления уполномоченного органа по защите прав субъектов персональных данных при соблюдении одного из следующих условий:

— персональные данные обрабатываются в соответствии с трудовым законодательством;

— персональные данные получены оператором в связи с заключением договора, стороной которого является субъект персональных данных, если персональные данные не распространяются (не предостав-

ляются третьим лицам) без согласия субъекта персональных данных и используются оператором исключительно для исполнения указанного договора и заключения договоров с субъектом персональных данных.

Автоматизированная обработка персональных данных на проходной

Современные СКУД состоят из программно-аппаратного комплекса, который позволяет среди прочего сканировать и распознавать документы посетителей предприятия, прикрепляя их к гостевой карте доступа (идентификатору). С технической точки зрения аппаратная часть контроллеры для СКУД обрабатывает и хранит только базу данных идентификаторов и, таким образом, не затрагивает персональных данных.

Именно в базе данных программного обеспечение для СКУД будут хранится как персональные данные сотрудников, так и посетителей. Современные программные комплексы по оформлению гостевых пропусков позволяют автоматизировать процесс ввода данных о посетителе. Как правило, это делает оператор на КПП, для оформления пропуска в организацию он производит сканирование паспорта, а иногда и дополнительно фотографирование посетителя. Эти данные вместе с данными о времени входа и выхода будут хранится в базе данных программного обеспечения» .

Ответственный за координацию работы системы контроля и управления доступом (СКУД) в образовательной организации обладает необходимыми полномочиями для определения политики выдачи пропусков, а также за обеспечение соблюдения положений правовых норм, регулирующих данную область. Кроме того, на данного ответственного возлагается задача осуществления контроля за соблюдением установленных требований. Ответственный за техническую поддержку системы контроля и управления доступом выполняет важную роль в обеспечении ее функционирования. В его обязанности входит замена и изъятие пропусков, а также оперативное решение эксплуатационных вопросов в рамках образовательной организации.

Для обеспечения эффективной системы оценки труда сотрудников необходимо реализовать ряд мероприятий, связанных с установлением стандартов эффективности работы для каждого рабочего места, а также разработкой критериев оценки. Кроме того, важным этапом является проведение оценки результативности труда, которая позволит определить вклад сотрудников в общий процесс производства, выявить наиболее эффективные рабочие места и уделять им особое внимание,

направить усилия на улучшение производительности труда и более эффективную организацию рабочего процесса.

В тесном взаимодействии со специалистами по персоналу можно разработать стратегии по сокращению расходов на обучение, повышению трудовой мотивации сотрудников, организации эффективной обратной связи по качеству работы и созданию программ обучения и развития персонала [6]. Все эти меры способствуют улучшению условий труда служащих предприятия и повышению их профессионального уровня, что позволит аккредитовать процесс оценки, обеспечить объективность и справедливость при ее проведении, определить лиц, ответственных за этот процесс, собрать необходимые данные, обсудить результаты оценки с работником, принять решения и документировать оценку.

Для этого следует определить функции, требования и произвести расчет общей оценки результативности, соответствующей стандартам, которые должны быть обобщены и переданы на рассмотрение подчиненному [5]. Эффективность оценки труда может быть достигнута путём установления понятных критериев для оцениваемого работника, эффективной системы оценки труда, которая обеспечивает свободный доступ к корректной и актуальной информации, используемой при процессе оценки и предоставления полного объяснения процедуры.

Заключение

При оценке эффективности труда необходимо учитывать фактор профессиональной этики в работе сотрудников. Для достижения эффективной системы оценки труда сотрудников необходимо обеспечить формирование общей культуры и профессиональных навыков, выражение профессиональной компетентности, эффективное использование средств и методов для достижения целей, а также рациональность. Применение профессиональной культуры, основанной на моральных нормах, и проявление профессиональной компетентности с учетом моральных установок способны стимулировать работников, у которых задачей является расширение возможностей для самореализации в профессиональном, личностном и гражданском плане. Эти основные факторы, сочетающие в себе этические и профессиональные аспекты, могут способствовать более полному восприятию и реализации процесса оценки труда.

Список источников

1. «Об утверждении порядка проведения классификации информационных систем персональных данных». Приказ ФСТЭК России, ФСБ

России, Мининформсвязи России от 13 февраля 2008 г. № 55/86/20 [Электронный ресурс] URL:https://27.rkn.gov.ru/docs/27/PRIKAZ_55_86_20.pdf (дата обращения 06.06.2023).

2. Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных» [Электронный ресурс] http://www.kremlin.ru/acts/bank/24154 (дата обращения 06.06.2023).

3. Положение об организации системы контроля и управления доступом (СКУД) при обеспечении контрольно-пропускного режима [Электронный ресурс] URL: https://www.tspk-mo.ru/storage/app/uploads/public/600/023/813/6000238138a52232434772.pdf (дата обращения 06.06.2023).

4. Виноградов В., Синюк А. Подготовка специалиста как человека культуры // Высшее образование в России.—№2.—2000.—С. 41.

5. Иванова И. В. Профессиональная культура управления: сущность, структура, динамика. М.: МГУ, 2007.—25 с.

6. Комбаров В. С. Профессиональная культура как способ реализации личности.—М.: изд-во МГУ, 2007.—21 с.

7. Мальцев А. Особенности обработки персональных данных в системах контроля и управления доступом. [Электронный ресурс] URL: http://www.techportal.ru/292846] (дата обращения 06.06.2023).

Об авторах

Федонин Александр Владимирович— студент 2 курса (магистратура) Института информационных наук; инженер-электроник отдела контрольно-пропускного режима, безопасности, антитеррористической и антикоррупционной деятельности Московского государственного лингвистического университета (Россия, Москва).
E-mail: avladimir2021@yandex.ru.

Гостев Александр Николаевич— доктор социологических наук, профессор, профессор кафедры информационной культуры цифровой трансформации, Московский государственный лингвистический университет (Россия, Москва).
E-mail: Gostevan@inbox.ru.

About the authors

Alexander V. Fedonin — 2nd year student (Master's degree) Institute of Information Sciences; Electronics Engineer of the Department of Checkpoint, Security, Anti-Terrorist and Anti-Corruption Activities of the Moscow State Linguistic University (Russia, Moscow).
E-mail: avladimir2021@yandex.ru.

Alexander N. Gostev— Doctor of Sociological Sciences, Professor, Professor of the Department of Information Culture of Digital Transformation, Moscow State Linguistic University (Russia, Moscow).
E-mail: Gostevan@inbox.ru.

УДК 004.056

НОРМАТИВНЫЕ ИНСТРУМЕНТЫ ЗАЩИТЫ ШКОЛЬНИКОВ ОТ ДЕСТРУКТИВНОГО КОНТЕНТА В ИНТЕРНЕТЕ

Хлебцова А. П.
Московский государственный лингвистический университет (Россия, Москва)
n.hleb@yandex.ru

Научный руководитель
Былевский П. Г.
Московский государственный лингвистический университет (Россия, Москва)
pr-911@yandex.ru

Аннотация

Поскольку современные дети все чаще пользуются интернет-сетью возрастает потребность в исследованиях, посвященных рискам, с которыми сталкиваются юные пользователи, а также тому, как следует с ними справляться. Эта статья собирает в себе различные исследования по негативному воздействию деструктивного контента и выдвигает предложения по созданию и модификации нормативных документов для обеспечения защиты школьников.

Ключевые слова

Деструктивный контент, школьники, социальные сети, нормативные инструменты.

Для цитирования: Хлебцова А. П. Нормативные инструменты защиты школьников от деструктивного контента в интернете // Hi-Hume Journal.—2023.—№ 1 (1).—С. 89—95.

REGULATORY TOOLS FOR PROTECTING SCHOOLCHILDREN FROM DESTRUCTIVE CONTENT ON THE INTERNET

Anastasia P. Khlebtsova
Moscow State Linguistic University (Moscow, Russia)
n.hleb@yandex.ru

Scientific supervisor
Pavel G. Bylevskiy
Moscow State Linguistic University (Russia, Moscow)
pr-911@yandex.ru

Abstract
As today's children increasingly use the Internet, there is a growing need for research on the risks young users face and how those risks should be managed. This article collects various studies on the negative impact of destructive content and puts forward proposals for the creation and modification of regulatory documents to ensure the protection of schoolchildren.

Key words
Destructive content, schoolchildren, social media, regulatory tools

For citation: Khlebtsova A. P. Regulatory tools for protecting schoolchildren from destructive content on the Internet // Hi-Hume Journal.—2023.—№ 1 (1).—Pp. 89—95.

Современная глобализация привела к развитию интернет-технологий и средств быстрого доступа к сети Интернет. Доступность киберпространства представляет собой интересный аспект, который в настоящее время является обычным явлением в учебных заведениях. Школьники не только имеют при себе персональные средства коммуникаций, такие как телефоны и планшеты, но и также имеют доступ глобальной сети через школьные компьютеры, по предоставленной школе сети wi-fi. Однако, никто не может быть уверенным, что неограниченный доступ к информации со всего мира не может нести в себе негативное влияние, которое может повлиять на формирующуюся психику школьников.

Признаками деструктивной информации являются:

1. Речевая агрессия, которая может быть выражена явно, а может являться скрытой;
2. Бесполезность предлагаемого контента. Нулевая смысловая нагрузка может также оказывать деградирующее воздействие на взрослых и детей;
3. Навязчивость одинаковой информации;
4. Пропаганда контента, призывающего к смерти, насилию, убийствам;
5. Искаженная информация и фальшивые новости [5].

Меры защиты учебных заведений от подобного контента в Интернете расписаны в документе "Правила подключения общеобразовательных учреждений к единой системе контент-фильтрации доступа к сети Интернет, реализованной Министерством образования и науки Российской Федерации" от 11 мая 2011 года № АФ-12/07 ВН, где говорится о средствах контент-фильтрации, которые должны быть установлены для ограничения интернет-доступа к информации, не рекомендуемой к просмотру несовершеннолетними.

Средства контент-фильтрации представляют собой устройство или программное обеспечение для фильтрации сайтов по их содержимому, не позволяющее получить доступ к определенным сайтам или услугам сети Интернет. Однако, рынок контент-фильтров очень большой, и не каждый из них подходит для защиты школ. Эта проблема в основном возникает из-за отсутствия регулирования аспекта выбора системы контент-фильтрации со стороны государства, так как сайт www.skf.edu.ru упомянутый в АФ-12/07 в данный момент недоступен, и администрация школ вынуждена сама принимать решение о выборе сетевого фильтра.

За последние годы в Российской федерации была проделана большая работа по формированию законодательных основ, направленных на обеспечение противодействия распространению вредоносной информации в том числе в сети Интернет. Например, Федеральный закон от 27 июля 2006 года № 149-ФЗ "Об информации, информационных технологиях и о защите информации" предусматривает государственное регулирование обеспечения информационной безопасности детей (п. 4 ч. 1 ст 12). Федеральный закон от 24 июля 1998 года № 124-ФЗ "Об основных гарантиях прав ребенка в Российской Федерации" устанавливает требования к распространению среди детей информации и обязывает органы государственной власти Российской Федерации осуществлять защиту ребенка от информации, пропаганды и агитации, наносящих вред его здоровью, нравственному и духовному развитию (ст. 14). Регулирование отношений, связанных с защитой детей от информации, причиняющей вред их здоровью и развитию описано в Федеральном законе № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»[4].

Также 24 ноября 2022 года в третьем чтении был принят закон о запрете пропаганды ЛГБТ, педофилии и смены пола среди несовершеннолетних, что несомненно добавит большое количество новых интернет-ресурсов в перечень запрещенных для доступа школьникам.

Однако без должного применения этих нормативных актов школьники остаются под сильным влиянием интернет-контента. Например,

согласно отдельной статистике, 99% учащихся пользуются Интернетом, проводят там от 2 до 6 часов в день, иногда и все 8 часов. Самыми популярными социальными сетями являются "ВКонтакте", "Инстаграм", "Одноклассники", "Твиттер" и "Телеграм" [4], все из которых имеют то или иное отношение к распространению деструктивного контента, включающего взрослый контент, сообщения о насилии, буллинг, суицидальные призывы и призывы асоциального поведения.

Согласно исследованию, из 528 страничек несовершеннолетних пользователей 103 (19,5%) сдержали девиантный контент: 44 аккаунта содержали аудио- и видеоматериалы, не соответствующие цензуре; 25—призыв к употреблению наркотиков, алкоголя или табака, 16—нецензурную брань в текстах и на видео; 14—контенты эротического содержания. Кроме того, на страницах учащихся выявлены аудио- и видеоматериалы, содержащие информацию о суициде, демонстрацию опасного хобби, пренебрежение правилам ПДД и пр. [4]. Это доказывает что в условиях отсутствия мер фильтрации контента, несовершеннолетние не только имеют к нему свободный доступ, но и распространяют его путем размещения на своей странице.

В другой статистике 92% школьников сталкиваются с деструктивным контентом в социальных сетях, а у больше половины школьников друзья или друзья знакомых состояли в группах деструктивной направленности [3]. Среди популярных игр, доступных в сети, преобладают симуляторы, игры военной тематики, а также игры со сценами насилия, жестокости—"Майнкрафт", "Варфрейм", "Тюряга" и другие [3]. В последней не только пропагандируется насилие и жестокость, но также и курение, употребление алкоголя, тюремных уставов и АУЕ (арестантский уклад един) тематик.

Мировые исследования также показывают что жертвами кибербуллинга среди детей и подростков оказываются около 20—40% [6]. При таких статистических показателях необходимость в методах ограничения доступа к запрещенному контенту становится очевидной.

На основе изученной нормативно-правовой базы в сфере обеспечения безопасности детей в сети "Интернет", были выявлены следующие проблемы:

1. Незаконное распространение порнографических материалов в сети Интернет оказывает травмирующее воздействие на психику детей и подростков. Важно отметить, что реклама такого рода очень слабо контролируется государством, так как по своим масштабам она огромна, и по статистике большинство запросов в Интернете связаны именно с этой тематикой.

2. Отсутствует правовое регулирование использования смартфонов школьниками. Закона, запрещающего ученикам всех школ Российской Федерации пользоваться телефонами в границах учебного заведения, нет. Федеральным законодательством установлен запрет на использование средств связи исключительно при проведении итоговой аттестации по образовательным программам основного общего и среднего общего образования. В то время как использование смартфонов в школьные будни не урегулировано.
3. Фильтрация, являющаяся основным механизмом защиты детей от вредоносного контента в Российской Федерации, не до конца выполняет свои задачи. Такие поисковые системы как Google и Яндекс недостаточно фильтруют запрещенный контент в поисковой выдаче. Без исключения запрещенных сайтов из поисковой выдачи дети и подростки могут увидеть сайты, побуждающие к насилию, суициду, пропаганде расовой/религиозной/этнической ненависти или вражды, а законодательство не регулирует валидность интернет-фильтров для школ.
4. Отсутствует обязательная возрастная идентификация пользователей в социальных сетях, что приводит к получению деструктивной, причиняющей вред здоровью и развитию ребенка, информации [5].
5. Персональные данные несовершеннолетних находятся в такой же опасности как и персональные данные взрослых [2]. Однако из-за их любопытства и желание проверить рамки дозволенности они могут чаще открывать подозрительные ссылки и сайты, чего можно было бы избежать при установке качественного контент-фильтра.

В связи со сложившейся ситуацией, целесообразно было бы применить нормативные меры:

1. Реализовать комплекс дополнительных предупредительных мероприятий, направленных на снижение деструктивной активности несовершеннолетних и выявление взрослых лиц, вовлекающих их в указанную деятельность с помощью сети Интернет [4].
2. Обеспечить постоянный мониторинг сети Интернет на предмет выявления вредоносной информации с последующим уведомлением Роскомнадзора для принятия мер, предусмотренных российским законодательством. Возможно даже создать сайт для принятия заявок о возможном деструктивном контенте, для их последующей обработки и оповещении провайдеров о необходимости блокировки ресурса, как это делает организация INHOPE [1].

3. Ввести обязательное включение в Устав образовательного учреждения ограничения (полного или частичного) по использованию средств связи в рамках образовательного процесса. То есть полностью или частично запретить учащимся использовать средства связи на уроках и внеклассных мероприятиях, исключения составляют лишь случаи, когда это необходимо для усвоения учебных дисциплин.
4. На законодательном уровне ввести обязательную возрастную идентификацию несовершеннолетних пользователей в социальных сетях.

В результате введения данного законопроекта, несовершеннолетние пользователи не будут получать информацию, не соответствующую их возрасту и нарушающую их психическое здоровье; [5] Подобные поправки к закону «О защите несовершеннолетних» вступили в силу с июня 2021 года в КНР. Согласно им, поставщики интернет-услуг должны внедрять средства для ограничения времени нахождения школьников в Сети. Подтверждение возраста производится с помощью государственной системы подтверждения личности пользователя [5]. В России такое ограничение может осуществляться через наличие у несовершеннолетнего паспорта или индивидуального школьного идентификатора.

Подобные мероприятия помогут повысить осведомленность об эмоциональном состоянии школьников, а также отследить цепочку появляющегося деструктивного контента и пресечь его дальнейшее распространение.

Выводы

Проведенный анализ показал, что несмотря на большую работу, проделанную над формированием нормативных инструментов для обеспечения защиты школьников от деструктивного контента в Интернете, существуют неопределенности их практического использования. Предлагаемые в этой статье меры могут помочь развитию нормативно-правовой базы и в дальнейшем обеспечить полную защиту школьников от возможного негативного воздействия в интернет-пространстве.

Список источников

1. Павленко И. В., Егорова В. С. Детская порнография в сети Интернет: состояние проблемы и мировые тенденции противодействия ей // Всероссийский криминологический журнал. 2021. Т. 15, № 1. С. 133-143.

2. Былевский П. Г. Пользовательские и персональные данные: анализ рисков «извлечения знаний» // Вопросы защиты информации.—2023.—№ 1—(140).—С. 35-40..

3. Друкер М. М. Медиапотреление современных подростков в условиях цифровой среды (на материале опроса старших школьников калининградской области)// Знак: проблемное поле медиаобразования. 2020. № 1 (35).—С. 15—24.

4. Герасимова Е. В., Жидконожкина О. Н. Социально-правовые аспекты профилактики правонарушений несовершеннолетних, совершаемых под воздействием деструктивных интернет-контентов.// Вестник Воронежского института МВД России.—2021—№ 1.— С. 265—270.

5. Симонова В. А., Лифинцева Е. А. Защита несовершеннолетних от негативной информации в сети интернет. // Научные известия.—2022.—№ 26.— С. 128—130.

6. Aboujaoude E., Savage M. W., Starcevic V., Salame W. O. Cyberbullying: Review of an old problem gone viral // Journal of Adolescent Health.—2015.—57 (1).—Pp. 10-18.

Об авторах

Хлебцова Анастасия Петровна—
студент 4 курса (бакалавриат) Института информационных наук Московского государственного лингвистического университета (Россия, Москва).
E-mail: n.hleb@yandex.ru.

Былевский Павел Геннадитвич—
кандидат философских наук, доцент; Московский государственный лингвистический университет (Россия, Москва).
E-mail: pr-911@yandex.ru.

About the authors

Anastasia P. Khlebtsova —
4th year student (bachelor's degree) Institute of Information Sciences, Moscow State Linguistic University (Russia, Moscow).
E-mail: n.hleb@yandex.ru.

Pavel G. Bylevskiy —
Candidate of Philosophical Sciences, Associate Professor; Moscow State Linguistic University (Russia, Moscow).
E-mail: pr-911@yandex.ru.

УДК 004.421+159.9.07

ФОРМИРОВАНИЕ ТРЕБОВАНИЙ К ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ ДЛЯ ВЫЯВЛЕНИЯ МАТЕМАТИЧЕСКИХ СПОСОБНОСТЕЙ У ОБУЧАЮЩИХСЯ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИИ ВИРТУАЛЬНОЙ РЕАЛЬНОСТИ

Самойлов В. Е.
Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации (Россия, Москва);
Московский государственный лингвистический университет (Россия, Москва)
samoilov.1992@list.ru

Ястребов Е. С.
Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации (Россия, Москва)
ceo@brainy-lab.com

Аннотация

В статье рассматриваются вопросы разработки общих требований, требований к технической документации и основного архитектурного решения. Для разработки общих требований проводится классификация методов выявления способностей обучающихся с помощью геймификации. Кроме того, в статье приводятся «узкие места», возникающие при разработке программного обеспечения с использованием технологий виртуальной реальности.

Ключевые слова

Компьютерная игра, психология, математические способности, алгоритмы диагностики, игровые механики.

Для цитирования: Самойлов В. Е., Ястребов Е. С. Формирование требований к программному обеспечению для выявления математических способностей у обучающихся с использованием технологии виртуальной реальности // Hi-Hume Journal.—2023.—№ 1 (1).—С. 96—103.

FORMATION OF SOFTWARE REQUIREMENTS FOR IDENTIFYING MATHEMATICAL ABILITIES OF STUDENTS USING VIRTUAL REALITY TECHNOLOGY

Vyacheslav E. Samoilov
Russian Academy of National Economy and Public Administration under the President of the Russian Federation (Moscow, Russia);
Moscow State Linguistic University (Moscow, Russia)
samoilov.1992@list.ru

Evgeny S. Yastrebov
Russian Presidential Academy of National Economy and Public Administration under the President of the Russian Federation Moscow, Russia)
ceo@brainy-lab.com

Abstract
The article deals with the development of general requirements, requirements for technical documentation and the main architectural solution. To develop general requirements, a classification of methods for identifying students' abilities using gamification is carried out. In addition, the article presents the "bottlenecks" that arise when developing software using virtual reality technologies.

Key words
Computer game, psychology, mathematical abilities, diagnostic algorithms, game mechanics.

For citation: Samoilov V. E., Yastrebov E. S. Formation of software requirements for identifying mathematical abilities in students using virtual reality technology // Hi-Hume Journal.—2023.—№ 1 (1).—Pp. 96—103.

Введение

С развитием технологий виртуальной реальности (ВР) появилась возможность создания уникальных образовательных сред, которые могут помочь в развитии математических способностей у детей.Программное обеспечение должно использовать различные сенсорные воз-

можности ВР для создания более полного и иммерсивного опыта обучения. Это может включать использование звука, тактильных ощущений и движений для повышения вовлеченности и улучшения понимания математических концепций.

С использованием геймификации в разных игровых сеттингах,а также элементов достижений (лидерские таблицы, награды) для стимулирования мотивации и интереса к изучению математики [3, 7]. Такой подход поможет создать более привлекательную, веселую образовательную среду. Для достижения эффективных результатов необходимо определить требования к программному обеспечению (ПО), которое будет использоваться для выявления и развития математических навыков и понимания у обучающихся.

Разработка общих требований к программному обеспечению

Интерфейс пользователя должен иметь интуитивно понятный и привлекательный интерфейс с использованием цветовых и звуковых сигналов для визуальной и аудиальной обратной связи. Важно предусмотреть возможность навигации в виртуальном пространстве с помощью удобных устройств управления, таких как контроллеры или жесты.

Разнообразный и структурированный контент, соответствующий уровню обучающихся. Покрывающий различные математические темы и концепции, предлагая задания и упражнения, адаптированные под уровень и потребности каждого обучающегося. Представленный в форме интерактивных сценариев, где обучающиеся могут взаимодействовать с объектами и оперировать математическими концепциями в виртуальном пространстве [1, 2].

Система аналитики, которая позволяет отслеживать и оценивать прогресс. Предоставлять детальную статистику о выполненных заданиях, достижениях, времени, затраченном на каждую задачу и другую информацию, необходимую для оценки эффективности. Что поможет учителям и родителям получить представление о развитии математических способностей.

Важно обеспечить конфиденциальность и безопасность данных, предусмотреть согласие родителей на использование ВР-технологии, а также обеспечить отсутствие дискриминации и стереотипов в контексте представленного контента и заданий:

- оценка результатов включает мгновенную обратную связь по выполнению заданий, объяснение правильных и неправильных ответов, статистику успехов и сложностей, а также рекомендации по дальнейшему обучению;

- мониторинг прогресса на протяжении всего времени позволит отслеживать изменения в способностях, определять области, требующие дополнительной поддержки, и адаптировать дальнейшее развитие в соответствии с индивидуальными потребностями;
- для развития пространственного мышления необходимо включать задачи на конструирование, решение головоломок с использованием пространственных представлений, визуализацию математических объектов в трехмерном пространстве и другие схожие задания.

Эти требования являются основой для разработки ПО, которое сможет эффективно выявлять и развивать математические способности с использованием технологии ВР. Учитывая требования, можно создать инновационные и эффективные инструменты, способствующие развитию математических способностей детей.

Классификация методов определения способностей

Исследование методов определения математических способностей у обучающихся показало, что с помощью подобного программного косвенным путем обеспечения могут быть выявлены также и другие способности ребенка.

Благодаря гибкости разрабатываемой игры и ВР технологиям туда можно заложить и другие тесты. Для абстрактного мышления—задачи на определение силы математической интуиции и воображения, а также манипуляции с абстракциями без опоры на конкретное.

Использование разрабатываемого программного обеспечения позволит проверить общую сообразительность и понимание общего восприятия поставленной задачи, а также физические данные, такие как скорость реакции. На *Схеме 1* представлена классификация методов определения способностей.

Схема 1. Классификация методов определения способностей

Требования к технической документации для реализации программного обеспечения

Геймдизайн документ (ГДД) должен включать такие разделы [5]:

1. **Общая концепция игры**—создать захватывающий волшебный мир, в котором игроки могут определить и развить свои способности, а также увлекательно проводить время в виртуальной реальности.

2. **Сеттинг и атмосфера** включает описание магического мира, представление различных локаций и персонажей, определение визуального стиля и атмосферы, разработку звукового оформления, проектирование пользовательского интерфейса и опыта, а также определение нарратива и задач игры, связанных с магическим миром и определение способностей.

3. **Игровые механики** включают в себя взаимодействие с магическими объектами, головоломки и задачами. Основная механика с учетом удобства использования и интуитивности, предоставляя игроку необходимые элементы управления и информационные панели.

4. **Уровни и прогрессия**—система уровней или локаций, которые игрок будет проходить в ходе путешествия. С описанием прогрессии игрока, включая разблокирование новых способностей, артефактов или улучшений.

5. **Геймплей и управление**—геймплей игры, включая описание действий игрока, реакции на его решения и взаимодействия. Как игрок будет управлять своим персонажем и магическими объектами с использованием контроллеров виртуальной реальности.

6. **Блок-схемы**—подробное описание действий игры для более четкого понимания предстоящего геймплея.

7. **Мультиплеер**—игра может иметь мультиплеерный режим, с возможностью соревнования и сотрудничества игроков в игровом мире.

8. **Графика и аудио**—требования к визуальному оформлению игры, включая дизайн персонажей, окружающей среды и специальных эффектов, а также аудиоэффекты и музыка, которые помогут создать атмосферу магического мира.

9. **Тестирование и балансировка**—план тестирования, включая проверку игровых механик, сложности головоломок и общего баланса игры. С возможностью обратной связи от игроков и внесение изменений на основе их отзывов.

10. **Расписание разработки и бюджет**—расписание разработки игры, включая этапы и сроки выполнения. С бюджетом проекта, включая затраты на разработку, графику, звук и тестирование.

11. **Лицензирование и защита прав**—на интеллектуальную собственность, включая ассоциированные с игрой персонажи, механики и идеи.

12. **Маркетинговые активности (Lifetime Value)**—дополнения в игре для удержания внимания и возвращения игроков

Выбор архитектурного решения для разработки игры в виртуальной реальности

Заключающим этапом перед началом разработки игры является выбор архитектурного решения [6, 8]. При использовании компьютерной игры для виртуальной реальности на мобильном шлеме Oculusquest 2 основную потерю ресурсов мощности будет уходить на реализацию графической части и поддержание FPS (framespersecond) выше 40 кадров в секунду для более плавного взаимодействия с виртуальным миром. Следовательно, будем использовать ограниченный набор графики.

Все данные игры будут собираться в памяти мобильного устройства и по завершению испытания будут отправлять на сервер в последующем будет проведен анализ и разработана нейросеть с помощью которой сложность в игре будет регулироваться и постепенно увеличиваться в зависимости от уровня прохождения и обучения игрока [4].

Шлем виртуальной реальности будет подключен к интернету через роутер по WIFI. Далее он отправляет данные на веб сервер через HTTP запрос (POST), по адресу API: api.brainy/games/vr/psytest. На веб сервере его принимает php скрипт, который обрабатывает данные и записывает их в БД, которая на том же физическом сервере [9].

На *Схеме 2* представлено изображение архитектуры системы.

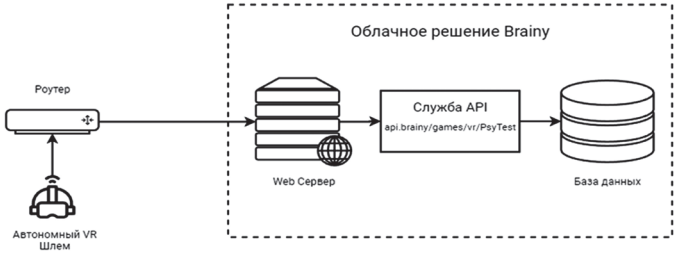

Схема 2. Архитектура системы

Заключение

При разработке любого программного обеспечения первым этапом становится проработка концепции и ее формализация. Проработка

концепции игры для выявления математических способностей у обучающихся показала, что важным является заинтересованность и вовлечение ребенка в игровой процесс, поэтому основной темой такой игры должна стать популярная вымышленная вселенная. Результаты анализа методов выявления способностей позволили построить классификацию и раскрыть возможность диагностирования дополнительных способностей — физических (скорость реакции) и абстрактных.

Сформированные требования к программному обеспечению позволят разработать игровые механики, способные с большей эффективностью (относительно психологических тестов) выявлять математические, абстрактные и физические способности детей.

Список источников

1. Лошкарева Д. А., Ваганова О. И., Макеева А. В. Методика проведения занятий с использованием интерактивных технологий обучения // проблемы современного педагогического образования. — 2018. — № 59-4. — С. 53-56.

2. Смирнов С. Д. Педагогика и психология высшего образования: от деятельности к личности. — М.: Аспект-пресс, 1995. — 270 с.

3. Ястребов Е. С. Корреляция восприятия обыденной и виртуальной реальностей в сознании человека / Е. С. Ястребов // Информационная безопасность и межкультурная коммуникация в контексте цифровой трансформации: Сборник научных трудов / Редакционная коллегия: П. Г. Былевский (отв. редактор) [и др.]. — Москва: Московский государственный лингвистический университет, Медиа Группа "Авангард", 2022. — С. 294-301. — EDN FZOXYU.

4. Huang W. H., Somanath S. Comparing the learning effectiveness of physical and virtual manipulatives in a mathematics lesson // International Journal of Science andMathematics Education. — 2013. — Vol. 11. — №3. — Pp/ 637-660.

5. Kebritchi M., Hirumi A., & Bai H. (2010). The Effects of Modern Math Computer Games on Learners' Math Achievement and Math Course Motivation in a Public High School Setting // Computers & Education. — Vol. 55. — №2. — Pp. 427-443.

6. Papastergiou M. Digital Game-Based Learning in high school Computer Science education: Impact on educational effectiveness and student motivation // Computers & Education. — 2009. — Vol. 52. — №1. — Pp. 1-12.

7. Samoilov V. E. Informative and Communicative Environment for the Development of Student Creativity and Flexible Skills / V. E. Samoilov, E. A. Bud-

nik, A. V. Tsaregorodtsev // Technology, Innovation and Creativity in Digital Society, St. Petersburg, 26–27 октября 2021 года. Vol. 345.—St. Petersburg: Springer Nature Switzerland, 2022.—P. 232-241.—DOI 10.1007/978-3-030-89708-6_20.—EDN YUFFTV.

8. Slater M., Sanchez-Vives, M. V. Enhancing Our Lives with Immersive Virtual Reality // Frontiersin Roboticsand AI.—2016.—Vol. 74. —№3. [Электронный ресурс] URL: https://www.frontiersin.org/articles/10.3389/frobt.2016.00074/full (дата обращения 2023.06.08).

9. Young M. F. Instructional Video Games: Young Minds in Focus / In R. E. Ferdig (Ed.), Handbook of Research on Effective Electronic Gaming in Educatio. Vol. I.—New York: Information Science Publishing, 2007. —Pp. 356-370.

Об авторах

Самойлов Вячеслав Евгеньевич—
кандидат технических наук, и. о. заведующего кафедрой международной информационной безопасности Института информационных наук Московского государственного лингвистического университета (Россия, Москва),
доцент кафедры системного анализа и информатики Российской академии народного хозяйства и государственной службы при Президенте РФ
(Россия, Москва).
E-mail: samoilov.1992@list.ru.

Ястребов Евгений Сергеевич—
студент 2 курса (магистратура)
Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации
(Россия, Москва).
E-mail: ceo@brainy-lab.com.

About the authors

Vyacheslav E. Samoilov —
Candidate of Technical Sciences,
Acting Head of the Department of International Information Security of the Institute of Information Sciences of the Moscow State Linguistic University (Moscow, Russia),
Associate Professor of the Department of System Analysis and Informatics of the Russian Presidential Academy of National Economy and Public Administration
(Russia, Moscow).
E-mail: samoilov.1992@list.ru.

Evgeny S. Yastrebov —
2nd year student (Master's degree)
The Russian Academy of National Economy and Public Administration under the President of the Russian Federation (Russia, Moscow).
E-mail: ceo@brainy-lab.com.

УДК 81

ИНТЕРПРЕТАЦИЯ И ЛИНГВОКРЕАТИВНОЕ КОНСТРУИРОВАНИЕ СВЯЗНОГО ТЕКСТА ПРИ ПЕРЕВОДЕ С АНГЛИЙСКОГО НА РУССКИЙ

Куковская А. В.
Московский государственный лингвистический университет (Россия, Москва)
a.kukovskaya@linguanet.ru

Аннотация

В статье исследуется проблематика, связанная с интерпретацией и порождением связного текста при переводе с английского на русский язык, основанном на лингвокреативном подходе. Материалом исследования послужил фрагмент размещенного в интернете текста, переведенный студентами-лингвистами 3-4 курсов, обучающимися в рамках программы дополнительного образования по письменному переводу с английского на русский язык. В статье анализируется, нарушение эквивалентности и адекватности перевода, связанное с неумением конструировать связный текст на ПЯ, соответствующий принципам когезии и когерентности. В статье формулируются выводы, сделанные в процессе исследования и анализа эмпирического материала и даются рекомендации по преодолению переводческих трудностей на основании лингвокреативного подхода.

Ключевые слова

Перевод, лингвокреативность, связность, когерентность, эквивалентность, адекватность, интерпретация текста

Для цитирования: Куковская А. В. Интерпретация и лингвокреативное конструирование связного текста при переводе с английского на русский // Hi-Hume Journal.—2023.—№ 1 (1).—С. 104—122.

INTERPRETATION AND LINGUOCREATIVE CONSTRUCTING A COHERENT TEXT WHEN TRANSLATING FROM ENGLISH TO RUSSIAN

Anna V. Kukovskaya
Moscow State Linguistic University (Moscow, Russia)
a.kukovskaya@linguanet.ru

Abstract

The article explores issues connected with the interpretation of ideas and the creation of a textual unity, characterized by cohesion and coherence, in the course of translation from English into Russian, based on linguistic creativity. As the material for the analysis served an online-posted fragment, translated by the third- and forth-year students of linguistics within the framework of the supplementary education course of written translation from English into Russian. The article analyzes how the violation of the equivalence and adequacy of translation is connected with the inability to create a coherent and cohesive text in the target language. The article formulates conclusions drawn in the process of research and the analysis of empirical material and provides recommendations for overcoming translation difficulties based on the linguistic creativity.

Key words

Translation, linguistic creativity, text cohesion, coherence, equivalence, adequacy, interpretation of ideas

For citation: Kukovskaya A.V. Interpretation and linguocreative construction of a coherent text when translated from English into Russian // Hi-Hume Journal.—2023.—№ 1 (1).—Pp. 104—122

Введение

Использование языка и его средств в повседневной жизни, в том числе при взаимодействии с переводом, неотделимо от лингвокреативного поведения человека [9; 10] и привносит в коммуникацию и язык новое, порождаемое на основании лингвокреативного мышления [9, p. 11; 8, p. 8, 81–82]. Современный человек, каждодневно общаясь, в том числе, в цифровом пространстве, имеет дело с конструированием различных текстов, как на родном, так и на иностранном языке. При этом переводчик должен способствовать успешной коммуникации и переводить англоязычные тексты различного характера, как в реальном общении, так и в пространстве блогосферы и интернета, где большинство текстов полимодально.

Поскольку мы опираемся на понимание перевода «как культурного и когнитивного явления», что предполагает его «интерпретацию как творческой деятельности» [7, с.7], особое внимание в статье уделяется

лингвокреативному аспекту в рамках конструирования адекватного и эквивалентного оригиналу связного текста на переводящем (русском) языке (ПЯ).

В цели и задачи настоящего исследования входит интерпретация текста на ИЯ (исходном языке) и анализ результатов его письменного перевода с английского на русский язык, а также предложение рекомендаций по созданию связного текста на ПЯ (переводящем языке) на сновании лингвокреативного подхода.

Актуальность исследования обусловлена интересом, который современная когнитивная лингвистка и переводоведение проявляют к поиску креативных инновационных подходов и переводческих решений, направленных на создание эквивалентных и адекватных оригиналу качественных связных текстов, в том числе представленных в англоязычном интернет-дискурсе. Необходимость разработки свежих эффективных подходов к переводу и интерпретации текста, опирающихся, в частности, на возможности лингвокреативного мышления, становится насущным требованием современности к профессиональному переводчику в условиях новой цифровой реальности, где нет монополии на конструирование текста и каждый пользователь имеет такую возможность.

Новизна исследования заключается в том, что трудности конструирования связных текстов в процессе их перевода в рамках лингвокреативного подхода изучены недостаточно.

Теоретической базой исследования послужили труды Н. Хомского и Р. Бервика по лингвистике и лингвокреативности, а также работы в области современного переводоведения таких авторов как В.Н. Комиссаров, Н.К. Рябцева, Н.А. Дудик, Е.В. Бреус, Д.В. Псурцев и др.

Практическая значимость исследования заключается в возможности использовать его для улучшения результатов интерпретации и перевода текстов, взятых как из интернет-дискурса, так и из иных сфер коммуникации. Также результаты исследования могут быть востребованы на практических занятиях и лекциях по переводу, на лекциях и семинарах по теории текста и дискурса, по лингвистике, при составлении учебных материалов по переводу с английского на русский язык. Полученные данные могут быть полезны при изучении затронутых вопросов на материале других языков, а рекомендации могут способствовать улучшению конструирования связных текстов при их письменном переводе с английского на русский язык.

Исследования базируется на следующем эмпирическом **материале**: мы предложили студентам-лингвистам 3-4 курсов, обучающимся

в рамках программы дополнительного образования по письменному переводу с английского на русский язык, перевести текст *«90 Minutes for America»*. Текст представлял собой открытое письмо, размещенное в интернете американскими деятелями культуры, в котором они призывали сограждан проголосовать на президентских выборах в США в 2012 году. Предполагалось, что студенты проведут предпереводческий анализ для лучшего понимания и адекватной интерпретации текста (включая ситуативный анализ политического контекста и общий анализ интернет-дискурса, из которого был взят текст), выстроят переводческую стратегию и предложат свой вариант перевода с английского на русский язык.

В процессе такой работы обучающиеся должны были опираться на освоенные теоретические знания, практические умения и навыки, соответствующие лингвистические и переводческие компетенции, а также на собственную способность к лингвокреативному мышлению. Все вышеперечисленное должно было позволить студентам представить в итоге качественный перевод в виде коммуникативно-равноценного оригиналу связного текста, отвечающего высоким требованиям адекватности и эквивалентности (при этом особый упор должен был быть сделан на прагматическую эквивалентность).

Конструирование связного текста на ПЯ: анализ трудностей и рекомендации по их преодолению

Оказалось, что самой распространенной трудностью, с которой столкнулись обучающиеся, является создание такого текста на ПЯ, который был бы **связным**, естественным (поскольку именно данная характеристика является «одной из самых замечательных характеристик перевода» [7 с. 7]), а также такого, который мог бы быть назван «эквивалентным оригиналу по смыслу и адекватным по средствам его выражения» [7, с. 57].

На первый взгляд представляется, что проблема конструирования связного текста с опорой на лингвокреативное мышление при переводе с английского на русский язык, не должна быть распространенной. Студенты-лингвисты обычно обладают рядом компетенций по лингвистической специальности и знакомы с теоретическими положениями о том, что связность («наличие смысловой или семантической связи между элементами и частями текста» [3, с. 32]) является неотъемлемой характеристикой любого текста.

При кратком опросе, нацеленном на выявление владения теоретическими знаниями, как правило, выясняется, что обучающиеся знакомы

с положениями о том, что «локальная связь (когезия)—это связь между отдельными элементами и частями текста, которая поверхностно (эксплицитно) выражается с помощью определенных языковых средств...». Здесь обычно выделяются такие языковые средства когезии как «наречия времени и места, временные формы глаголов, лексические повторы, синонимы, союзы, указательные слова или местоимения» [3, с. 32]. А глобальная связность (когерентность), осуществляемая на уровне всего текста, имеет отношение к экстралингвистическим знаниям—о фрагменте реальности, о котором говорится в тексте, о ситуации, в которой происходит общение»; когерентность «обеспечивается общностью темы, пространственно-временными, причинно-следственными связями…, общностью целей автора» [3, с. 32].

Но даже имея теоретические познания, студенты, как показало наше исследование, либо не достигли автоматизации соответствующих навыком и умений для применения знаний на практике, либо нетвердо усвоили тот факт, что «когерентность осуществляется на уровне всего текста» [3, с. 32]. Следовательно, несмотря на то, что студенты применили отдельные переводческие приемы и трансформации, некоторые из которых являлись результатом их лингвокреативного мышления, представленные варианты перевода в большинстве случаев не стали качественными. Конструируя текст, студенты, затруднялись реализовать на практике свое знание теории, забывая о том, что текст на ПЯ должен быть естественным, адекватным (т. е. «выступать в качестве полноценной замены текста оригинала» [2, с. 11]) и эквивалентным на уровнях, «обеспечивающих то же прагматическое воздействие на получателя информации, что и текст оригинала» [2, с. 11]), а главное, связным.

Представляется, что подобная ситуация складывается в результате сочетания ошибок при выстраивании стратегии перевода, при проведении предпереводческого анализа и при непосредственном выполнении перевода. Это комплексная проблема, проистекающая из отсутствия автоматизации базовых лингвистических навыков, недостаточного (в случае некоторых студентов) владения ИЯ и/или ПЯ, неумения соотнести теорию с практикой и/или отсутствия необходимого объема практики (отработки приемов и навыков), а главное, из пристрастия к буквализму, возникающему «когда при сохранении синтаксиса или семантики оригинала прагматическая эквивалентность не достигается» [6, с. 14].

Студентам, особенно на начальных этапах обучения переводу, достаточно трудно нарушить буквальное соответствие на нижних уровнях

эквивалентности (синтаксическом, лексическом и т. д.) ради сохранения прагматики, вследствие чего перевод остается «недотрансформированным», не обретает естественности и не может быть оценен как адекватный или оптимизированный относительно уровней эквивалентности. Иными словами, студенты, выполняя перевод, обычно начинают анализ и выстраивают стратегию, начиная с нижних уровней эквивалентности (морфологического, лексического, семантического, синтаксического), с преобразования на уровне отдельного предложения (или даже слова и/или словосочетания). Такой «подстрочный» подход приводит к тому, что переводя слова, студенты забывают о необходимости передавать общий смысл, а полученный текст на ПЯ теряет связность, присущую оригиналу.

Для устранения этой комплексной ошибки следует заострить внимание на том, что предложение, являясь «минимальным речевым произведением» должно пониматься не как «грамматическое предложение», а как «высказывание», лишь по форме совпадающее с таким предложением, но «включенное в конкретную речевую ситуацию и имеющее конкретное коммуникативное задание» [2, с. 20]. Иными словами, выполняя перевод, следует стремиться уйти от буквализма и сфокусироваться на эквивалентности, на прагматике и на уровне текста. Также необходимо помнить, что переводчик «имеет дело с текстами», и поэтому «для перевода существенной является эквивалентность значения не отдельных слов и даже не изолированных предложений, а всего переводимого текста» [2, с. 19]. Нижние уровни эквивалентности должны подстраиваться под высшие, но не наоборот, поскольку «прагматическая эквивалентность может существовать без семантической и без синтаксической» [6, с.8].

Нам представляется, что создание перевода с последующим его обсуждением на занятии, сравнение предложенных студентами стратегий перевода и версий, а также, что особенно важно, сопоставление текстов (фрагментов текстов) оригинала и перевода, будет успешной тактикой преодоления описанных выше трудностей, связанных с получением связного текста при выполнении перевода. Как отмечают исследователи и педагоги, «сопоставление текста на ИЯ и ПЯ важно для того, чтобы привлечь внимание обучающихся к различию форм выражения одних и тех же смыслов в родном и иностранном языке» [2, с. 13]. Такой подход также поможет активизировать лингвокреативное мышление, что, в свою очередь, может расширить арсенал приемов и подходов, используемых при переводе и подсказать неожиданные, но успешные решения и варианты интерпретации текста.

Конструирование связного текста при переводе: интерпретация и предпереводческий анализ текста

Ниже представлен фрагмент оригинала данного текста на английском языке:

«Dear America,

We humbly ask our fans to not watch our TV shows or movies, or listen to our music tonight. We ask you, instead, to invest 90 minutes in our country, and watch the first debate between President Barack Obama and Governor Mitt Romney.

The differences between these two men and the Republican and Democratic party policies in 2012 are enormous.

And exciting.

Never before has there been this kind of opportunity for Americans to choose such vastly different philosophies, priorities, values and direction for our country. We, truly, get to Choose our America on November 6.

And, it is really easy.»

(URL: https://www.huffpost.com/entry/first-presidential-debate_b_1936056)

Прежде всего, поскольку данный публицистический текст (обладающий вербальными и невербальными особенностями) был опубликован в интернете и представляет собой прямое обращение деятелей культуры США к согражданам. Текст сочетает в себе черты письменной и устной речи, актуализированные при помощи визуального (форматирование) и вербального модусов. При интерпретации данного отрезка текста следует учитывать общий публицистико-политический контекст представленного фрагмента текста: его авторы призывают сограждан выполнить гражданский долг, пойти на выборы и обязательно посмотреть перед этим дебаты между кандидатами в президенты США.

С визуальной точки зрения обращает на себя внимание форматирование текста и его разбивка на абзацы: она не случайна, поскольку имеет место повторение приема парцелляции, служащей для стилистического выделения значимых для авторов мыслей в публицистическом тексте. В рамках реализации прагматической задачи авторы текста прибегают не только к стилистическим приемам, но и к выразительным средствам. Прагматическая установка авторов заключается в желании завлечь избирателей на выборы. Обращает на себя внимание коммуникативная стратегия , реализующая эту установку: американцам говорят, что выборы—это не только волнующе и интересно, но и крайне просто. Это достигаетися за счет выразительных языковых средств: различия между предвыборными обещаниями называются в тексте не только «огром-

ными\существенными» *(enormous)*, но и «интересными, волнующими, будоражащими» *(exciting)*, а сам процесс выбора президента и участия в выборах характеризуется словосочетанием «очень просто» *(really easy)*. Причем именно характеристики «*exciting*» и «*really easy*» выделены особо при помощи стилистических и графических приемов.

Идея простоты подчеркивается своеобразной литотой, когда авторы предпочитают написать «*90 minutes*» вместо «полтора часа», видимо полагая, что отрезок времени, выраженный в минутах воспримется читателями как более короткий, чем он же, выраженный в часах. Кроме того, стоит отметить параллелизм в конструкции исходного текста, наблюдаемый в устно-письменном интернет-дискурсе, в том числе, визуально: короткие абзацы чередуются с длинными.

При этом с прагматической и смысловой точки зрения короткие абзацы являются центром коммуникации, в них реализуются стилистические приемы, нацеленные на оказание наибольшего влияния на читателя. Чтобы заинтересовать читателей выборами и обеспечить их явку, авторы, в рамках своей прагматической задачи, чередуют призывы и пояснения с подчеркиванием установки, что выборы—это интересно, просто и на благо Америки. Фактически, данный текст может быть схематично представлен в виде ключевых узлов, отвечающих авторской прагматической задаче и отражающих коммуникативную стратегию (выделение наше):

«*Dear America,...*

...And exciting.

...And, it is really easy.»

Деятели культуры (известные актеры, певцы, режиссеры и т.п.) обращаются к избирателям «*Dear America*», что, при всей очевидной клишированности и формальности, уважительно ставит последних в более высокое положение (особенно в сочетании с употреблением слова «смиренно» в выражении «*We* ***humbly*** *ask our fans*» в первом абзаце). Одновременно такое обращение намекает, что избиратели являются единой общностью—американцами, гражданами единой Америки, которых деятели культуры смиренно просят об услуге, которая, при всей ее важности, интересна и проста в исполнении. Общность американцев как граждан Америки и важность их миссии—гражданского долга участвовать в выборах—подчеркивается стилистическими повторами «*Dear America*», «*our country*», «*opportunity for Americans*», «*get to Choose our America*». Неоднократное употребление местоимения «our» в отношении граждан Америки служит целям как когезии, так и когерентности, а также позволяет авторам, в рамках их коммуникативной

стратегии и реализации прегматических задач, подчеркнуть свою связь с теми, к кому они обращаются.

Американцев смиренно и даже самоуничижительно просят не смотреть созданные деятелями культуры (и по-совместительству авторами открытого письма) шоу или слушать написанную ими музыку, утверждая, что эти достижения в области искусства менее важны, чем гражданский долг участия в выборах.

Не менее важны когезия и когерентность, представленные в тексте на ИЯ стилистически окрашенными синонимичными единицами, принадлежащими к семантическому полю, связанному с выборами и возможностями, выбором и будущим: «*invest*», «*opportunity*», «*choose*», «*philosophies*», «*priorities*», «*value*», «*direction*», «*get to Choose*» (здесь также обращает на себя внимание заглавнfz буквf, актуализированнfz при помощи визуального модуса).

Когезия в данном стилистически окрашенном за счет указанных приемов фрагменте характеризуется не только упомянутыми выше лексическими повторами и синонимами *(«America», «our country»)*, но и лексическим повтором в сочетании с параллельной конструкцией «*We humbly* ***ask our fans to not*** *watch our TV shows or movies, or listen to our music tonight.* ***We ask you, instead****...*». Связность места и времени во фрагменте подчеркивается формами глаголов (употребленных во временах настоящего времени «*are enormous*», «*has there been*»), противопоставлением наречий «*tonight*», «*never before*» в сочетании с эмфатической инверсией «***Never before has there been*** *this kind of opportunity for Americans to choose...*». Также когезия манифестируется через повторение союзов в парцеллированных и начинающихся с новых строк параллельных конструкций «*And exciting*», «*And, it is really easy*».

Все эти факторы когезии помогают авторам актуализировать связность и на уровне когерентности всего текста на уровне прагматической задачи в рамках коммуникативной стратегии. Очевидно, что при переводе данную интерпретацию оригинала необходимо сохранить и передать на ПЯ, как минимум на прагматическом уровне, а в лучшем случае с сохранением стилистических приемов оригинала и его визуальной архитектуры. Иначе перевод не будет коммуникативно-равноценным.

Конструирование связного текста при переводе: анализ ошибок

Итак, рассмотрим указанные выше ключевые узлы оригинала, соответствующие им отрывки и конкретные примеры письменного перевода с английского на русский язык.

Ниже представлен первый отрывок и несколько вариантов, представленных студентами (выделение наше, орфография и прочие особенности сохранены), в данном случае обращая внимание на перевод выделенных элементов (выделение наше), поскольку именно передача связности текста при переводе находится в фокусе нашего внимания:

Оригинал отрывка 1 (первый ключевой узел):

«***Dear America***,

We humbly ask our fans to not watch our TV shows or movies, or ***listen to our*** *music tonight. We ask* ***you****, instead, to invest 90 minutes* ***in our country****...»*

Повторение местоимения «our» (что может рассматриваться как стилистический прием) в отношении американцев служит прагматическим задачам авторов (подчеркнуть тот факт, что они все — граждане одной страны, от которых зависит их общее будущее) и отвечает принципам конструирования текста на принципах когезии и когерентности.

Примеры перевода отрывка 1:

1.1. *«Дорогая* ***Америка****!*

Мы покорно просим наших телезрителей и радиослушателей сегодня вечером отказаться от просмотра ***телепередач, фильмов*** *и прослушивания* ***музыки****. Вместо этого, мы просим* ***Вас*** *уделить 90 минут и сделать вклад в* ***нашу*** *страну...».*

1.2. *«Дорогие американцы,*

Мы смиренно просим ***своих*** *поклонников не смотреть ТВ шоу, фильмы и не слушать музыку сегодня вечером. Вместо этого вложите 90 минут* ***вашего*** *времени в* ***нашу*** *страну...»*

Примеры 1.1-2 представляют собой типичный вариант недотрансформированного буквального (подстрочного) перевода, не отвечающего требованиям эквивалентности и адекватности вследствие множественных недочетов и нарушения нормы ПЯ. Также очевидно, что в примерах 1.1-2 проигнорирован принцип связности, как на уровне когезии, так и на уровне когерентности: нет связи между обращением «Америка» и последующим призывом к телезрителям-американцам. Более того, сочетание данного обращения с буквальным переводом фразы *«We ask you»* и местоимения в выражении ***«in our country»*** как *«**в нашу** страну»* создает впечатление, что авторы обращения — граждане иной страны и не являются американцами, которых при этом просят вкладываться в некую неназванную родину авторов.

Здесь очевидно нарушение эквивалентности и адекватности по причине непонимания студентом того факта, что в текст на ПЯ необходимо конструировать, переводя предложения не изолировано поотдельности, а следуя принципам когерентности, чтобы правильно

передать идею оригинала: «американцы обращаются к согражданам ради блага Америки». К этому же типу нарушения связности относится неуместное употребление *«Вас»* с заглавной буквы, вредящее связности текста в том, что касается передачи идеи общности народа и обращения к американцам как к единой нации.

Пропуск притяжательного местоимения в словосочетании *«просмотра **телепередач, фильмов** и прослушивания **музыки**»* (ср. оригинал *«watch **our** TV shows or movies, or **listen to our** music»*) также является смысловым недочетом, имеющим отношение к непониманию должны моделироваться на ПЯ тексты на основе когезии и когерентности. В данном случае опущение притяжательного местоимения разрушает мысль оригинала о том, что деятели культуры смирено (покорно) просят зрителей вместо просмотра ИХ произведений уделить внимание просмотру дебатов. Опущение местоимения нарушает связность текста и, следовательно разрушает его смысл.

Пример **1.3**: *«Дорогие **американцы**!*

*Мы смиренно просим **наших** фанатов сегодня вечером не смотреть **наши** телешоу и фильмы и не слушать **нашу** музыку. Вместо этого мы просим **вас** посвятить 90 минут вашего времени будущему **нашей** страны...».*

Пример **1.4**: *«Дорогие **граждане Америки**,*

*Сегодня вечером мы покорно просим наших телезрителей не проводить время за просмотром наших телевизионных шоу, фильмов и прослушиванием **нашей** музыки. Вместо этого мы просим **вас** потратить эти 90 минут на **нашу** страну...».*

Примеры 1.3-4 в какой-то мере исправляют ошибки Примеров 1.1-2. Повторение притяжательного местоимения *«our»* отвечает прагматическим установкам авторов текста и, следовательно, в ПЯ может также рассматриваться как намеренный стилистический прием. Употребление в обращении существительного *«американцы»* и *«граждане Америки»* также представляется удачным переводческим решением. Тем не менее, в данных примерах также можно наблюдать нарушение связности в том смысле, что в ПЯ нарушается глобальная когерентность на уровне логических связей, поскольку на языковом уровне нарушается когезия, и студентам не удается нормативными средствами русского языка выразить мысль текста на ИЯ, заключающуюся в том, что здесь американцы из обращения и есть это те зрители, которых просят не смотреть один вечер шоу и т. п., но посвятить время просмотру дебатов ради общего будущего Америки, гражданами которой авторы письма и его адресаты совместно являются.

Из примеров 1.1-4 создается впечатление, что это все разные группы и разные страны.

Также, стоит отметить, что перевод Примеров 1.3-4 не может быть охарактеризован как продукт лингвокреативного подхода: присутствующая в них некоторая связность представляется формальной, возникшей в результате старательного, но во многом буквального перевода и калькирования в ПЯ конструкций ИЯ.

Например, на основании лингвокреативного мышления для подчеркивания когерентности и эксплицитного выражения когезии на языковом уровне можно было бы написать (вариант создан студентами по результатам работы над ошибками): «*Дорогие* ***американцы****! Мы смиренно обращаемся к,* ***вам, нашим*** *фанатам:* ***вместо того****, чтобы сегодня вечером смотреть* ***наши*** *телешоу и фильмы* ***или*** *слушать* ***нашу*** *музыку, мы просим* ***вас*** *посвятить 90 минут* ***вашего*** *времени будущему* ***нашей общей*** *страны...* ». Несмотря на некоторую вольность, а также нарушение рабочего уровня эквивалентности на лексическом и синтаксическом уровнях, данный вариант перевода сохраняет прагматическую эквивалентность и адекватность, оставаясь при этом связным как в плане языка, так и в плане имплицитных идей. Также в таком варианте обращает на себя внимание достаточно успешная попытка сохранить в ПЯ стилистические приемы оригинала.

Так, наша рекомендация заключается в том, что, в тех случаях, когда лингвокреативный подход приводит к вольности в переводе, надо руководствоваться утверждением, что «свободный перевод может быть признан адекватным, если он отвечает другим нормативным требованиям перевода и не связан с существенными потерями в передаче содержания оригинала… . серьезные отклонения от содержания оригинала делают свободный перевод неэквивалентным и неадекватным, превращая его в «переложение» или самостоятельное высказывание на тему оригинала» [4, с.235].

Рассмотрим отрывок 2 оригинала (второй ключевой узел): «***The differences*** *between these two men and the Republican and Democratic party policies in 2012* ***are enormous.***

And exciting».

Несомненно, что здесь мы имеем дело со сверхфразовым единством (СФЕ), в котором присутствует разбивка не только на предложения, но и на абзацы для усиления окрашенности при помощи парцелляции, подкрепленной графическим форматированием (когезия на уровне визуального модуса), но которое, при этом выражает единую мысль, подчеркнутую вышеуказанными приемами.

Примеры 2.1-10 перевода отрывка 2:

2.1. «*В 2012 году между этими двумя личностями и их партиями* ***существуют огромные различия.***

И волнительны».

2..2 «*В 2012 году между этими двумя лидерами и политикой Республиканской и Демократической партий* ***существуют огромные различия.***

И волнительные».

2..3. «*Между этими двумя людьми, как и между политическими взглядами Республиканской и Демократической партиями в 2012 году,* ***огромная разница.***

И захватывающая».

2..4. «***Различия*** *между этими двумя политиками, а также политикой Республиканской и Демократической партий в 2012 году* ***огромны. И не менее волнительны***».

2..5. «*В 2012 году* ***различия*** *между программами этих политиков и стратегиями Республиканской и Демократической партий* ***были довольно значительными.***

Мы бы даже сказали будоражащими».

2..6. «***Различия*** *между двумя этими людьми, как и между политикой Республиканской и Демократической партий в 2012 году,* ***огромны.***

И именно поэтому захватывающи».

2..7. «***Различия*** *между этими людьми и политикой республиканской и демократической партии в 2012 году огромны.*

А наиболее волнующий факт —

Для американцев доныне не представлялась такого рода возможность выбора диаметральных философий, приоритетов, ценностей и направлений развития для нашей страны».

2..8. «***Различия*** *между политиками, как и между программами Республиканской и Демократической партий в 2012 году,* ***колоссальные****.*

Порой даже впечатляющие».

2..9. «***Пропасть*** *между этими мужчинами, а также между политикой республиканской партии и Партии демократов в 2012 году,* ***просто огромна.***

Это будоражи*т*».

2..10. «***Ведь различия*** *между этими двумя политиками, а также между программами Республиканской и Демократической партий в 2012 году* ***поистине колоссальны.***

И это самое интересное».

На первых взгляд, во всех вариантах, кроме 2.1. (где нарушается не просто связность текста, но даже формальное грамматическое согласо-

вание «***...существуют огромные различия. И волнительны***»), присутствует, по меньшей мере, попытка соединить предложения и абзацы в СФЕ и представить связный на уровне когезии и когерентности текст на ПЯ. Однако, в примерах 2.2-3 связность представляется формальной, возникающей автоматически за счет перевода с ИЯ на ПЯ такого языкового средства когезии, как союз: «***...существуют огромные различия. И волнительные***», «***...огромная разница. И захватывающая***». В данных примерах мы видим недотрансформированный, буквальный перевод, при конструировании которого студент не задумывался ни о связности в рамках СФЕ, ни тем более на уровне всего текста. Естественно, в случае примеров 2.1-3 речь о лингвокреативном подходе не идет—формальный подход к переводу данного фрагмента исключает активизирование лингвокреативного мышления.

Наоборот, в примерах 2.4-10 присутствует попытка сохранения связности на уровне когезии и когерентности, основанная на лингвокреативном подходе: перевод во всех примерах разный, что доказывает активизирование лингвокреативного мышления при конструировании связного текста на ПЯ. Обращает на себя пример 2.4. (***Различия… огромны. И не менее волнительны***)—в нем лингвокреативный подход привел к вольности: студент объединил абзацы, разъединенные в оригинале. И хотя такой прием допустим, а в некоторых случаях даже желателен [2], в данном случае такая стратегия результируется в отказе от сохранения внешних характеристик (переданных при помощи визуального модуса) опубликованного в интернете оригинала текста. Перевод теряет значимые характеристики оригинала.

И, хотя известно, что «во имя передачи главного и существенного в исходном тексте (его коммуникативной установки) переводчику нередко приходится идти на известные жертвы и потери» [1, с. 57], и что «творческий, основанный на лингвокреативности, подход к переводу… текста должен стать приоритетным выбором при определении переводческой стратегии», следует учитывать, что «не всегда при таком подходе достигается эквивалентность и адекватность, а перевод, кажущийся вполне «хорошим» может содержать в себе значительные искажения» [5, с. 347].

Примеры 2.5-10 представляют собой реализацию лингвокреативного подхода при попытке сохранить связность текста на ПЯ. Имплицитная когерентность достигается здесь достаточно удачно за счет средств эксплицитной когезии на языковом уровне. Однако вольность в переводе не представляется полностью удачной. Так, в примерах 2.5 и 2.8 мы видим прием добавления лексических единиц («*Мы бы даже сказали...*»,

«Порой даже...») для упрочнения когезии на уровне языка, однако нам представляется, что это не до конца оправданная вольность, искажающая смысл оригинала на лексическом уровне.

Интересен пример 2.7.: в нем студент делает попытку сохранить связность текста, но привязывает фразу «*And exciting*», которую передает как «*А наиболее волнующий факт—»* к следующему, а не к предыдущему абзацу. Такую логику нельзя совсем исключить, ибо анализируемый фрагмент на ИЯ представляет собой хорошо продуманный целиком связный текст (и волнительный интерес может объясняться как различиями в политических взглядах, там и наличием беспрецедентных возможностей сделать выбор).

Однако синтаксис оригинала и стилистический прием (фраза «*And exciting*» совершенно очевидно отделена от предыдущего предложения и вынесена в отдельный абзац в рамках приема эмфатической парцелляции) доказывают, что данная фраза все-таки сильнее связана с предыдущим, а не с последующим абзацем.

Пример 2.6. с вариантом «*...И именно поэтому захватывающи*» также моет служить иллюстрацией успешной попытки сохранить когерентность за счет эксплицитной когезии на языковом уровне на ПЯ: студент выносит из подтекста в текст причинно-логическую связь. Но недочет заключается в том, что в оригинале данная причинно-следственная связь отсутствует.

Различия в политических взглядах называются существенными (*enormous*) и интересными (*exciting*), однако не утверждается, что они интересны *потому что* огромны. И поскольку «главным критерием оценки переводческой деятельности, а также адекватности и эквивалентности перевода является коммуникативная равноценность» [5, с. 347], можно утверждать, что здесь также имеет место вольность, приводящая к искажению, хотя и проистекающая из попытки сохранения связности текста.

Примеры 2.9-10, таким образом, представляются наиболее удачной реализацией лингвокреативного подхода к сохранению когезии и когерентности оригинала, поскольку передавая связность текста на ПЯ они успешно используют переводческие трансформации и добиваются прагматической эквивалентности и адекватности, учитывают особенности текста на английском (даже визуальный аспект; но, к сожалению, почти теряют парцелляцию, особенно пример 2.9).

Рассмотрим отрывок 3 оригинала (первый ключевой узел):

*«We, truly, **get to Choose our America** on November 6.*

*And, it is **really easy**».*

Примеры 3.1-5 перевода отрывка 3 (орфография и т. п. сохранены):

3.1. «*6 ноября мы* ***действительно выберем нашу Америку****.*

И это ***действительно несложно****»*.

3.2. «*6 ноября мы* ***действительно выбираем Нашу Америку****.*

И это, ***поистине, очень просто****»*.

3.3. «*6 ноября мы,* ***действительно****, выбираем дальнейший путь развития Америки.*

И, ***на самом деле, процесс не сложен****»*.

3.4.. «*6 ноября мы сможем* ***по-настоящему выбрать будущее Америки****.*

Всё ***просто****»*.

3.5. «***Голосование*** *состоится 6 ноября.*

Что может быть ***проще?****»*.

Неумение сконструировать связный текст очевидно в примерах 3.1-3, что проявляется в повторении синонимичных выражений «действительно», «на самом деле», утяжеляющих текст. Такая избыточность тавтологична на ПЯ и является маркером буквального перевода. Предложения переводились не как связное СФЕ, а по-отдельности, без учета тема-тематических отношений и без попытки эмфатически выделить центр коммуникации, предположим, за счет изменения порядка слов (например, вынесения «действительно» в начало первого предложения).

Пример 3.2. представляет собой попытку исправить недотрансформированный и нарушающий нормы ПЯ (тавтология) пример 3.1 путем применения лингвокреативного подхода. Это манифестируется в примере 3.2. не только в попытке творчески подойти к переводу второго предложения и использовать стилистические окрашенное наречие «*поистине*», но также в использовании графических средств (визуального модуса)—вместо заглавной буквы в слове «*Choose*» студент использует ее в притяжательном местоимении «*Нашу*».

Пример 3.3. идет дальше по пути лингвокреативности (можно отметить, например, антонимический перевод «*easy*»—«*не сложен*»). В примере вместо местоимения «*это*» употребляет существительное «*процесс*», что может рассматриваться как попытка применения приема логической синонимии или, возможно, конкретизации. С одной стороны, это манифестирует стремление сохранить связность текста: студент имел в виду, что в контексте «*процесс*»—это выборы в широком смысле. С другой стороны, такое употребление неудачно и нарушает логические связи внутри текста на уровне когерентности, т. к. в рамках порожденного в ПЯ СФЕ («*6 ноября мы,* ***действительно****, выбираем дальнейший путь развития Америки. И,* ***на самом деле, процесс не сложен****»*) складывается впечатление, что «*процесс*» здесь—это «путь развития Америки»

(так происходит в результате нарушения когезии вследствие нарушения норм ПЯ: поскольку существительное «*процесс*», по мнению студента, должно заменить глагол «*выбираем*», хотя, по правилам русского языка, оно служит здесь синонимом существительного «*развитие*», что и создает смысловое искажение).

Примеры 3.4-5 основаны на лингвокреативном подходе и являются более вольными.

В 3.5. наблюдается изменение типа предложения и ряд иных переводческих трансформаций (опущение, модуляция), в результате которых появляется слово «*голосование*».

В 3.4. удачным представляется выбор творческого переводческого решения, позволивший студенту создать следующее СФЕ: «*6 ноября мы сможем* ***по-настоящему выбрать будущее Америки***. *Всё* ***просто***». Представляется, что прием опущения способствует сохранению связности текста как в плане когезии на уровне языка, так и в плане когерентности. Решение эксплицитно не повторять во втором предложении мысль, выраженную в первом передложении наречием «по-настоящему» способствует смысловому спаиванию отрывка, что обеспечивает его коммуникативную равноценность оригиналу.

Заключение

Таким образом, анализ теоретических предпосылок исследования и эмпирического материала позволяет сделать ряд выводов о проблематике, связанной с конструированием связного текста при переводе с английского на русский язык. Корень проблемы кроется в том, что многие начинающиеся переводчики не рассматривают тексты на ИЯ как единое целое, обладающее внешними (ну уровне языка) и внутренними (на уровне логических связей и идей) связями, и продолжают переводить их, в лучшем случае, как разрозненные предложения или, в худшем, как отдельные слова.

Это приводит к возникновению недотрансформированного буквального (подстрочного) перевода, нарушающего нормы русского языка. В таких неудачных переводах на ПЯ нарушается когезия и когерентность, вследствие чего они не могут быть признаны эквивалентными или адекватными. Фактически, из-за отсутствия в них связности они не могут быть признаны текстами.

Поскольку, как показало наше исследование, отсутствие связности в переводах студентов, является, как правило, следствием опасения отклониться в сторону вольности и, как следствие, результатом проявле-

ния излишнего буквализма, то одним из возможных вариантов решения данной проблемы является опора на лингвокреативный подход. Такой подход может раскрыть творческий потенциал переводчика, показать ему креативные возможности языка. Вторым необходимым компонентом решения проблемы является, вероятно, более тщательный подход к предпереводческому анализу текста на ИЯ, к интерпретации заключенных в нем идей и внутренних логических и т.п. связей, с последующим переложением их на ПЯ в виде коммуникативно-равноценного связного текста, характеризующегося эквивалентностью и адекватностью.

Список источников

1. Бреус Е. В. Введение в теорию и практику письменного англо-русского перевода (на материале публицистических текстов). Учеб.пособие.—М.: ФГБОУ ВПО МГЛУ, 2013.—282 с.

2. Дудик Н. А. Конструирование текста на переводящем языке при переводе с русского языка на английский язык. Часть I. Учебн.пособие.—М.: ФГБОУ ВПО МГЛУ, 2012.—144 с.

3. Ирисханова О. К. Лингвистика in brevi: Учеб.пособие для студентов начальных курсов.—М.: ИПК МГЛУ «Рема», 2012.—96 с.

4. Комиссаров В. Н. Теория перевода (лингвистические аспекты): Учеб.для ин-тов и фак. иностр. яз.—М.: Высш. шк., 1990.—253 с.

5. Куковская А. В. Лингвокреативное конструирование текста как фактор нарушения эквивалентности в переводе // Информационная безопасность и межкультурная коммуникация в контексте цифровой трансформации. Сборник научных трудов. Редакционная коллегия: П.Г. Былевский (отв. редактор) [и др.].—М.: Московский государственный лингвистический университет, Медиа Группа «Авангард», 2022.—С. 346-351.

6. Псурцев Д. В. Стратегия перевода: учеб. пособие по письменному переводу с английского языка на русский для студентов V курса.—М.: Рема, 2010.—160 с.

7. Рябцева Н. К. Прикладные проблемы переводоведения: Лингвистический аспект: учеб. пособие. –М.: Флинта; Наука, 2016.—224 с.

8. Berwick R. C., Chomsky N. Why only us: language and evolution. Cambridge: The MIT Press, 2016.—215 p.

9. Chomsky N. Language and mind. Cambridge: Cambridge University Press, 2016.—190 p.

10. Chomsky N. What kind of creatures are we? New York: Columbia University Press, 2016.—167 p.

Об авторе

Куковская Анна Владимировна— старший преподаватель кафедры лингвистики и профессиональной коммуникации в области информационных наук Института информационных наук Московского государственного лингвистического университета
(Россия, Москва).
E-mail: a.kukovskaya@linguanet.ru.

About the author

Anna V. Kukovskaya —
Senior Lecturer, Department of Linguistics and Professional Communication in the Field of Information Sciences, Institute of Information Sciences, Moscow State Linguistic University
(Russia, Moscow).
E-mail: a.kukovskaya@linguanet.ru.

УДК 04.94 + 372.881.1

РАЗРАБОТКА МОДЕЛИ БАЗЫ ДАННЫХ КОМПЬЮТЕРНОЙ ИГРЫ ДЛЯ ОБУЧЕНИЯ ИНОСТРАННЫМ ЯЗЫКАМ С ПРИМЕНЕНИЕМ ТЕХНОЛОГИЙ ВИРТУАЛЬНОЙ РЕАЛЬНОСТИ

Еремина-Драчева Ю. М.
Российская академия народного хозяйства и государственной службы
при Президенте Российской Федерации(Россия, Москва)
yudracheva@gmail.com

Научный руководитель
Самойлов В. Е.
Российская академия народного хозяйства и государственной службы
при Президенте Российской Федерации (Россия, Москва);
Московский государственный лингвистический университет (Россия, Москва)
samoilov.1992@list.ru

Аннотация
В статье приводится разработка модели базы данных компьютерной игры для обучения иностранным языкам с применением технологий виртуальной реальности.

Ключевые слова
Модель базы данных, компьютерная игра, UML

Для цитирования: Еремина-Драчева Ю. М. Разработка модели базы данных компьютерной игры для обучения иностранным языкам с применением технологий виртуальной реальности // Hi-Hume Journal.—2023.—№ 1 (1).—С. 123—132.

DEVELOPMENT OF A COMPUTER GAME DATABASE MODEL FOR TEACHING FOREIGN LANGUAGE USING VIRTUAL REALITY TECHNOLOGY

Iuliia M. Eremina-Dracheva
The Russian Presidential Academy of National Economy
and Public Administration (Moscow, Russia)
yudracheva@gmail.com

Scientific supervisor
Samoilov V. E.
Russian Academy of National Economy and Public Administration
under the President of the Russian Federation (Russia, Moscow);
Moscow State Linguistic University (Moscow, Russia)
samoilov.1992@list.ru

Abstract
This article provides the development of a computer game database model for foreign language teaching using virtual reality technologies.

Key words
Database model, computer game, UML

For citation: Eremina-Dracheva Yu. M. Development of a database model of a computer game for teaching foreign languages using virtual reality technologies // Hi-Hume Journal.—2023.—№ 1 (1).—Pp. 123—132.

Введение

При разработке компьютерной игры для обучения иностранным языкам с применением технологий виртуальной реальности было необходимо разработать модель базы данных для хранения информации по пользователям и изучаемым словам.

Выбор методов и средств разработки модели базы данных

При проектировании базы данных можно также использовать модели UML, и по результату получаются эффективные, согласованные и легко расширяемые системы [1]. Первоначально стоит проанализировать модели предметной области. В том числе для базы данных были использованы реляционные СУБД, потому что они более удобные и доступные на рынке [8]. Реляционные базы данных хранят данные в виде таблиц с определенной структурой [5, 6]. Каждая таблица имеет конкретное количество столбцов с определенным типом и произвольное число строк.

При формировании таблиц реляционных баз данных, стоит учитывать согласованность их содержимого [3]. Данная операция поможет

уменьшить избыточность данных и повысить производительность базы данных. Для формирования структуры описания данных также использовалось бесплатное программное средство Diagrams.net [2]. Данное веб-приложение очень удобное для проектирования UML диаграмм.

Разработка логической модели базы данных

При проектировании структурограммы описания данных, первоначально стоит разработать классы объектов, которые используются в компьютерной игре и сервисах [7]. Список классов изображен на Схеме 1.

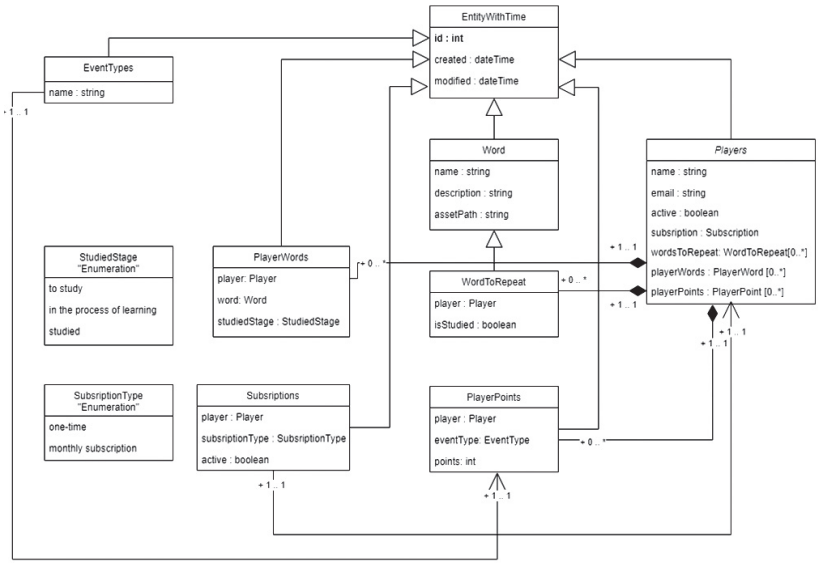

Схема 1. Диаграмма классов

Сущности «Слово», «Слово для повторения», «Пользователи», «Очки пользователя» и «Подписки» имеют одинаковые поля «Идентификатор», «Дата создания» и «Дата изменения», поэтому была выделена отдельная сущность «Сущность со временем», от которой наследуются ранее перечисленные сущности.

При проектировании были выделены сущности логического уровня и их определения, которые описаны в Таблице 1. При создании таблиц в базе данных, как правило, стоит их именовать с помощью латиницы, поэтому в данной таблице также представлено английское наименование сущностей [4].

Таблица 1. Сущности и их определения

Наименование сущности	**Английское наименование сущности**	**Определение**
Слова	Words	Содержит все существующие слова, которые могут встретиться в игре
Слова для повторения	Words to repeat	Содержит слова, которые игрок должен повторить
Слова пользователя	Player words	Содержит слова, с которыми игрок уже знаком
Типы события	Event types	Содержит типы событий, за которые игрок получил баллы
Пользователи	Players	Содержит список всех игроков
Очки пользователя	Player points	Содержит историю получения баллов
Подписки	Subscriptions	Содержит пользовательские подписки
Типы подписок	Subscription types	Содержит типы подписок

Данные об отношениях между таблицами представлены в Таблице 2.

Таблица 2. Отношения между таблицами

Родительская сущность	**Дочерняя сущность**	**Имя связи**	**Тип связи**	**Семантика связи от родительской сущности к дочерней**
Слова	Слова для повторения	Слов-Пов	НИД 1:М	включает
Слова	Слова пользователя	Слов-СлПол	ИД 1:М	содержат
Очки пользователя	Типы события	Оч-ТипСоб	ИД М:М	содержат
Пользователи	Очки пользователя	Пол-Оч	ИД М:М	создают
Пользователи	Слова пользователя	Пол-СлПол	ИД 1:М	выбирают
Подписки	Пользователи	Под-Пол	ИД 1:1	покупают
Подписки	Типы подписки	Под-ТипПод	ИД М:1	имеют

В результате была сформирована ER-диаграмма, которая изображена на Схеме 2.

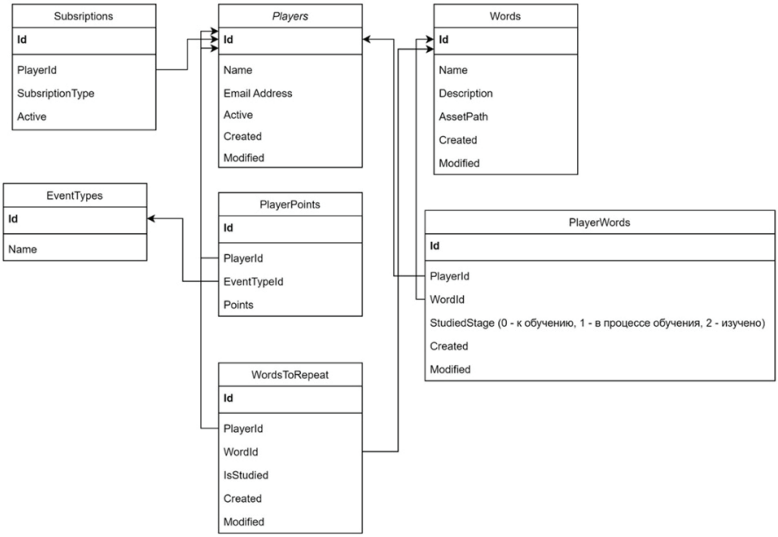

Схема 2. Структура базы данных

Помимо сущностей и связей, модель данных включает в себя ключевые атрибуты сущностей, такие как первичные (PK) и внешние ключи (FK).

На основание данных требований были установлены следующие первичные и внешние ключи:

1. Каждому слову соответствует уникальный идентификатор.

2. Каждому слову на повторения соответствует уникальный идентификатор.

3. Каждое слово на повторение соответствует определенное слово из таблицы «Слова».

4. Каждое слово на повторение соответствует какому-либо пользователю.

5. Каждому слову пользователя соответствует уникальный идентификатор.

6. Каждое слово пользователя соответствует определенное слово из таблицы «Слова».

7. Каждое слово пользователя соответствует какому-либо пользователю.

8. Каждому пользователю соответствует уникальный идентификатор.

9. Каждому заработанному очку пользователя соответствует уникальный идентификатор.

10. Каждому типу события соответствует уникальный идентификатор.

11. Каждая запись о заработанных очках соответствует тип события.

12. Каждой подписке соответствует уникальный идентификатор.

13. Каждый пользователь имеет подписку.

14. Каждому типы подписки соответствует уникальный идентификатор.

15. Каждая подписка имеет тип.

Полная атрибутивная модель представляет данные в четвертой НФ и включает все сущности, атрибуты и связи.

В Таблице 3 отображены атрибуты выявленных ранее сущностей и их описание.

Таблица 3. Атрибуты сущностей

Имя сущности	**Описание атрибутов**			
	Наименование атрибута	**Желаемое сокращение атрибута**	**Ключи**	**Возможно ли неопределенное значение**
Слова	Идентификатор	Id	PK	Нет
	Наименование	Name		Нет
	Описание	Description		Да
	Путь до картинки	AssetPath		Да
	Дата создания	Created		Нет
	Дата последнего изменения	Modified		Нет
Слова для повторения	Идентификатор	Id	PK	Нет
	Идентификатор пользователя	PlayerId	FK	Нет
	Идентификатор слова	WordId	FK	Нет
	Признак изученности	IsStudied		Да
	Дата создания	Created		Нет
	Дата последнего изменения	Modified		Нет
Слова пользователя	Идентификатор	Id	PK	Нет
	Идентификатор пользователя	PlayerId	FK	Нет
	Идентификатор слова	WordId	FK	Нет
	Состояние изучения	StudiedStage		Нет
	Дата создания	Created		Нет
	Дата последнего изменения	Modified		Нет
Типы события	Идентификатор	Id	PK	Нет
	Наименование	Name		Нет

Имя сущности	Описание атрибутов			
	Наименование атрибута	Желаемое сокращение атрибута	Ключи	Возможно ли неопределенное значение
	Наименование	Name		Нет
	Электронный адрес	Email		Нет
	Активность	Active		Нет
	Дата создания	Created		Нет
	Дата последнего изменения	Modified		Нет
Очки пользователя	Идентификатор	Id	PK	Нет
	Идентификатор пользователя	PlayerId	FK	Нет
	Тип события	EventTypeId	FK	Нет
	Очки	Points		Нет
	Дата создания	Created		Нет
	Дата последнего изменения	Modified		Нет
Подписки	Идентификатор	Id	PK	Нет
	Идентификатор пользователя	PlayerId	FK	Нет
	Тип подписки	SubscriptionTypeId	FK	Нет
	Активность	Active		Нет
Типы подписок	Идентификатор	Id	PK	Нет
	Наименование	Name		Нет

Разработка физической модели базы данных

Формирование физической модели базы данных зависит от конкретной СУБД. В Microsoft Azure, где будет опубликована база данных, присутствует возможность использовать Microsoft SQL Server и MySQL [9, 10]. Данные базы данных имеют практически одинаковую структуру, поэтому сформированную физическую модели можно использовать для всех выше перечисленных СУБД. Для формирования Т-модели были сформированы домены атрибутов сущностей, области и допустимых значений и типы данных (Таблица №4).

Таблица 4. Данные для Т-модели

Шифр домена	Тип	Определение	Пример
D1	Int(11)	Целое числовое значение	54781
D2	DateTime	Дата в формате ДД.ММ.ГГГГ ЧЧ:ММ:СС	20.11.2023 15:45:23
D3	Boolean	Истина или ложь	ИСТИНА
D4	VARCHAR (100)	Набор символов, количество которых не превышает 100	Морозова Екатерина Ивановна
D5	VARCHAR (500)	Набор символов, количество которых не превышает 500	Длинный текст
D6	CHAR (18)	Набор символов, число которых не превышает 18	2

Далее необходимо присвоить текущим атрибутам сущностей сформированные домены атрибутов. Присвоение изображено в таблице 5.

Таблица 5. Присвоение атрибутам сущностей сформированные домены атрибутов

Имя сущности	**Описание атрибутов**	
	Наименование атрибута	**Шифр домена**
Слова	Идентификатор	D1
	Наименование	D4
	Описание	D5
	Путь до картинки	D4
	Дата создания	D2
	Дата последнего изменения	D2
Слова для повторения	Идентификатор	D1
	Идентификатор пользователя	D1
	Идентификатор слова	D1
	Признак изученности	D3
	Дата создания	D2
	Дата последнего изменения	D2
Слова пользователя	Идентификатор	D1
	Идентификатор пользователя	D1
	Идентификатор слова	D1
	Состояние изучения	D6
	Дата создания	D2
	Дата последнего изменения	D2
Типы события	Идентификатор	D1
	Наименование	D4
Пользователи	Идентификатор	D1
	Наименование	D4
	Электронный адрес	D4
	Активность	D3
	Дата создания	D2
	Дата последнего изменения	D2
Очки пользователя	Идентификатор	D1
	Идентификатор пользователя	D1
	Тип события	D1
	Очки	D1
	Дата создания	D2
	Дата последнего изменения	D2
Подписки	Идентификатор	D1
	Идентификатор пользователя	D1
	Тип подписки	D1
	Активность	D3
Типы подписок	Идентификатор	D1
	Наименование	D4

Заключение

Разработанная модель базы данных была применена в компьютерной игре LanguageAdventureVR, которая на момент написания статьи находится на стадии разработки.

Список источников

1. Буйволов Е. А. Сравнение производительности современных NOSQL баз данных с реляционной базой данных Sybase ASA 9.02 / Е. А. Буйволов // Проблемы науки.—2020.—№ 6(54).—С. 26-30.—DOI 10.24411/2413-2101-2020-10601.—EDN HIQXAD.

2. Веселов Д. И. Обзор онлайн-сервисов по созданию инфографики для учебного процесса / Д. И. Веселов, В. Б. Порутчиков, В. А. Семиглазов // Инноватика-2022 : Сборник материалов XVIII международной школы-конференции студентов, аспирантов и молодых ученых, Томск, 21–22 апреля 2022 года.—Томск: Общество с ограниченной ответственностью «СТТ», 2022.—С. 462-465.—EDN PYYQVO.

3. Карпова И. П. Базы данных: курс лекций и материалы для практических занятий: учебное пособие для студентов технических факультетов, изучающих автоматизированные информационные системы и системы управления базами данных. М.: ИД «Питер», 2013.—240 с.

4. Михайличенко А. // Правила именования объектов базы данных. 28 April 2023. URL: http://citforum.ru/database/articles/naming_rule

5. Моисеев В. В. Начальная модель данных предметной области на основе реляционной базы данных / В. В. Моисеев, Н. Г. Ярушкина // Автоматизация процессов управления.—2019.—№ 4(58).—С. 51-56.—DOI 10.35752/1991-2927-2019-4-58-51-56.—EDN XSKEYI.

6. Основы проектирования реляционных баз данных // НОУ «ИНТУИТ». 2023, April 24. [Электронный ресурс] URL: https://intuit.ru/studies/professional_skill_improvements/1754/courses/191/lecture/4969?page=2 (дата обращения 06.06.2023).

7. Плакса Ю. А., Силантьев А. Б., Анисимов О. В., Близнюк. О. Н. Информатика: Учеб. пособие.– Ярославль: Типография ВУНЦ ВВС «ВВА» (филиал, г. Ярославль), 2011.—437 с.—EDN ZUVFMB.

8. Рамбо Дж., Блаха М. UML 2.0. Объектно-ориентированное моделирование и разработка.—2-е изд.—СПб.: Питер, 2007.—544 с.

9. Azure // Microsoft. 2023, April 24 [Электронный ресурс] URL: https://azure.microsoft.com (дата обращения 06.06.2023).

10. Singh N., Kehoe M. Cloud Native Infrastructure with Azure: Building and Managing Cloud Native Applications 1st Edition.—Cambridge: O'Reilly Media, Inc., 2022.—324 p.

Об авторах

Еремина-Драчева Юлия Максимовна— студент 2-го курса (магистратура) Российской академии народного хозяйства и государственной службы при Президенте РФ (Россия, Москва).
E-mail: yudracheva@gmail.com.

Самойлов Вячеслав Евгеньевич— кандидат технических наук, и. о. заведующего кафедрой международной информационной безопасности Института информационных наук Московского государственного лингвистического университета (Россия, Москва), доцент кафедры системного анализа и информатики Российской академии народного хозяйства и государственной службы при Президенте РФ (Россия, Москва).
E-mail: samoilov.1992@list.ru.

About the authors

Yulia M. Yeremina-Dracheva — 2nd year student (Master's degree) Russian Academy of National Economy and Public Administration under the President of the Russian Federation (Russia, Moscow).
E-mail: yudracheva@gmail.com.

Vyacheslav E. Samoilov — Candidate of Technical Sciences, Acting Head of the Department of International Information Security of the Institute of Information Sciences of the Moscow State Linguistic University (Moscow, Russia), Associate Professor of the Department of System Analysis and Informatics of the Russian Presidential Academy of National Economy and Public Administration (Russia, Moscow).
E-mail: samoilov.1992@list.ru.

УДК 001.89

АНАЛИЗ ДОСТУПНОСТИ В ЭЛЕКТРОННОМ ВИДЕ НАУЧНЫХ ПЕРИОДИЧЕСКИХ ИЗДАНИЙ ПО ФИЛОЛОГИИ, ОТНЕСЕННЫХ К ПЕРВОЙ КАТЕГОРИИ ПЕРЕЧНЯ ВАК

Романова С. А.
Московский государственный лингвистический университет (Россия, Москва)
s.a.romanova@linguanet.ru

Аннотация
В данной статье анализируется наличие доступа к электронным вариантам выпусков научных периодических изданий по филологии, включенных в Перечень ВАК и соотнесенных с первой категорией по итогам работы экспертной группы ВАК Министерства науки и высшего образования РФ в 2022 году.

Ключевые слова
Научное периодическое издание, первая категория, перечень ВАК, открытый доступ, филология.

Для цитирования: Романова С. А. Анализ доступности в электронном виде научных периодических изданий по филологии, отнесенных к первой категории Перечня ВАК // Hi-Hume Journal.—2023.—№ 1 (1).—С.133—144.

ANALYSIS OF THE AVAILABILITY IN ELECTRONIC FORM OF SCIENTIFIC PERIODICALS ON PHILOLOGY, CLASSIFIED IN THE FIRST CATEGORY OF THE LIST OF THE HIGHER ATTESTATION COMMISSION

Svetlana A. Romanova
Moscow State Linguistic University (Moscow, Russia)
s.a.romanova@linguanet.ru

Abstract

This article analyzes the availability of access to electronic versions of issues of scientific periodicals on philology included in the List of the Higher Attestation Commission and correlated with the first category according to the results of the work of the expert group Higher Attestation Commission of the Ministry of Science and Higher Education of the Russian Federation in 2022.

Keywords

Scientific periodical, first category, list of the Higher Attestation Commission, open access, philology.

For citation: Romanova S. A. Analysis of the availability in electronic form of scientific periodicals on philology, classified in the first category of the List of the Higher Attestation Commission // Hi-Hume Journal.—2023.—№ 1 (1).—P. 133—144.

Постановка проблемы

В связи с постоянно растущим количеством научных периодических изданий и проводимых исследований по филологическим наукам возникла потребность в анализе доступности подготавливаемых на высоком редакционном и научном уровне публикаций в изданиях, отнесенных к первой категории Перечня ВАК по филологическим наукам. К апрелю 2023 года в Перечне ВАК появилось 41 новое издание по филологическим наукам или смежным с ними дисциплинам.

Исследователям при аргументации своей научной точки зрения необходимо опираться на достоверные и точные результаты исследований коллег. Источником достоверных и точных данных являются в первую очередь исследовательские статьи [2, с. 72] из научных периодических изданий, прошедшие редактирование, рецензирование и рассмотренные на заседаниях редакционных коллегий. (Иными источниками служат также монографии, препринты, репозитории исследовательских данных).

Степень доступности источников данных определяет темпы развития науки. Чем больше научных статей, отнесенных в том числе и к первой категории Перечня ВАК, находится в открытом доступе в электронном виде, тем больше у исследователя возможностей ознакомиться с ними подробно и корректно их процитировать, согласиться или опровергнуть их позицию.

В октябре 2022 года Высшая аттестационная комиссия Министерства науки и высшего образования Российской Федерации в рекомендации № 2-пл/1 [1] определила новые критерии оценки публикационной активности для соискателей ученых степеней, кандидатов и докторов наук, членов диссертационных советов, которые вводятся с 1 сентября 2023 года. Позднее в декабре 2022 года научной общественности было представлено информационное письмо ВАК Минобрнауки России «О Перечне рецензируемых научных изданий» [2] с приложением о распределении научных периодических изданий по трем категориям К1, К2, К3 на основании проведенной экспертной группой оценки всех изданий, включенных в Перечень ВАК в 2021 году. Методика распределения изданий по категориям подробно описана в работе [3, с. 7-8].

Как следует из рекомендации ВАК № 2-пл/1, для создания, возобновления или внесения изменений в состав диссертационного совета, их членам необходимо иметь публикации в научных периодических изданиях первой и второй категории Перечня ВАК наравне с публикациями из изданий, включенных в RSCI, отнесенных к Q-1 или Q-2 в международных базах данных.

В 2021 году научные специальности (в том числе по филологии) были укрупнены для того, чтобы способствовать междисциплинарным исследованиям аспирантов и докторантов и соответствовать темпам развития науки. Некоторые научные специальности и группы научных специальностей сократились, при этом появились новые научные специальности (см. подробно [1]). Также были пересмотрены и утверждены новые паспорта научных специальностей [3].

---

[1] См.: Рекомендация ВАК Минобрнауки России от 26 октября 2022 года № 2-пл/1 «О новых критериях к соискателям ученых степеней кандидата наук, доктора наук, к членам диссертационных советов» [Электронный ресурс] // URL: https://vak.minobrnauki.gov.ru/uploader/loader?type=35&name=92246639002&f=13999 (дата обращения: 05.05.2023).

[2] См.: Информационное письмо Высшей аттестационной комиссии при Министерстве науки и высшего образования Российской Федерации от 6 декабря 2022 г. № 02-1198 «О Перечне рецензируемых научных изданий» [Электронный ресурс] // URL: https://vak.minobrnauki.gov.ru/uploader/loader?type=19&name=92263438002&f=14239 (дата обращения: 05.03.2023).

[3] См.: Паспорта научных специальностей номенклатуры научных специальностей, по которым присуждаются ученые степени, утвержденной приказом Министерства науки и высшего образования Российской Федерации от 24 февраля 2021 г. № 118 // URL: https://nppir.com/pasporta-vak/ (дата обращения: 05.05.2023).

Согласно приказу Минобрнауки России от 24 февраля 2021 года №118 [4] к новой группе специальностей по филологии отнесены следующие научные специальности: 5.9.1.—Русская литература и литературы народов Российской Федерации; 5.9.2.—Литературы народов мира; 5.9.3.—Теория литературы; 5.9.4.—Фольклористика; 5.9.5.—Русский язык. Языки народов России; 5.9.6. Языки народов зарубежных стран (с указанием конкретного языка или группы языков); 5.9.7.—Классическая, византийская и новогреческая филология; 5.9.8.—Теоретическая, прикладная и сравнительно-сопоставительная лингвистика; 5.9.9.—Медиакоммуникации и журналистика; 5.12.3—Междисциплинарные исследования языка (филологические науки).

Интерпретация полученных результатов

Распределение изданий по вышеперечисленным специальностям показало, что в Перечень ВАК по состоянию на апрель 2023 года [5] включены 250 научных периодических изданий, принимающих статьи по филологическим наукам.

В настоящем исследовании анализируются 42 издания, отнесенные экспертной группой к первой категории Перечня ВАК и прошедшие переаккредитацию по новым научным специальностям по филологическим наукам (см. Приложение 1) по критерию «доступности» архивов выпусков.

Другие 208 научных периодических изданий детально не анализировались в виду различных изменений в их статусе за прошедшие 2 года с момента их экспертной оценки. Например, за 2022-2023 начали издаваться новые издания—41; не прошли переаккредитацию по новым научным специальностям—5 изданий; отнесены к К2 108 изданий; от-

[4] См.: Приказ Министерства науки и высшего образования Российской Федерации от 24 февраля 2021 г. № 118 «Об утверждении номенклатуры научных специальностей, по которым присуждаются ученые степени, и внесении изменения в Положение о совете по защите диссертаций на соискание ученой степени кандидата наук, на соискание ученой степени доктора наук, утвержденное приказом Министерства образования и науки Российской Федерации от 10 ноября 2017 г. № 1093» (Зарегистрирован в Минюсте России 06.04.2021 № 62998) (ред. от 20.12.2022). // URL: https://www.consultant.ru/document/cons_doc_LAW_381578/ (дата обращения: 05.05.2023).

[5] См.: Перечень рецензируемых научных изданий, в которых должны быть опубликованы основные научные результаты диссертаций на соискание ученой степени кандидата наук, на соискание ученой степени доктора наук (по состоянию на 25.04.2023) [Электронный ресурс] // URL: https://vak.minobrnauki.gov.ru/uploader/loader?type=19&name=91107547002&f=17883 (дата обращения: 05.05.2023).

несены к К3 54 издания; включены в Scopus или Web of Science и их категория должна быть изменена на К1 согласно рекомендации ВАК № 2-пл/1—8 изданий.

В первую очередь был изучен уровень доступа к архивным выпускам 42 изданий, отнесенных к К1. Под «доступностью» мы подразумеваем размещение электронной версии статьи (чаще в формате pdf) в открытом, бесплатном доступе для исследователя на сайте издания, на сайте вуза или в НЭБ «Elibrary.ru». Доступ к статье в электронном виде открыт круглосуточно [4, с. 112] при наличии доступа в интернет у исследователя и функционировании сайта электронного книгохранилища (библиотеки, репозитория).

В случае же взимания платы за электронную версию статьи доступ считается закрытым, платным, но в то же время доступ к оплате и получении статьи в сети интернет круглосуточный. Если издатель открыл доступ к архивам выпусков, а текущие выпуски находятся в закрытом, платном доступе, тогда такой вариант доступа называется «гибридным».

Анализ доступности показал, что с открытым доступом выпускается 39 научных периодических изданий, с платным доступом к архивам и текущим номерам—1 издание, в гибридном доступе—2 издания.

Затем был рассмотрен статус учредителя издания. Так, 29 научных периодических изданий выпускаются российскими образовательными организациями; 8—РАН; 4—коммерческими организациями; у одного издания смешанный состав учредителей (РАН и российские образовательные организации).

Образовательные организации размещают выпуски своих изданий в открытом доступе как на сайте издания, так и в НЭБ «Elibrary.ru». За принятие в такое издание статьи к опубликованию плата не взимается. Коммерческие организации, наоборот, взимают плату с авторов за редакционные услуги. Исключением является редакция издания «Вопросы когнитивной лингвистики», принимающая статьи на безвозмездной основе.

Дополнительно были соотнесены виды доступа к архивам с научными специальностями, по которым издание прошло переаккредитацию. Данные представлены в Таблице 1.

Как видно из приведенной таблицы, исследователю предоставлен открытый доступ более чем к 92 % публикуемых статей по всем новым научным специальностям по филологическим наукам, что позволяет ему обосновать научную новизну, теоретическую значимость своего исследования и корректно процитировать первоисточник.

Таблица 1. Распределение научных периодических изданий первой категории Перечня ВАК по филологическим специальностям в зависимости от доступа к выпускам

Критерии доступа к выпускам	**Научные специальности**									
	5.9.1.	5.9.2.	5.9.3.	5.9.4.	5.9.5.	5.9.6.	5.9.7.	5.9.8.	5.9.9.	5.12.3.
С платным доступом ко всем выпускам	1	1	1	0	1	1	0	1	1	1
С бесплатным доступом ко всем выпускам	21	12	18	12	29	18	5	29	11	5
Гибридный доступ	1	1	1	0	1	0	1	1	0	0
Число научных периодических изданий первой категории из Перечня ВАК (всего)	23	14	20	12	31	19	6	31	12	6

Выводы и обсуждения

Продолжается работа научного сообщества по предоставлению открытого доступа к статьям научных периодических изданий или препринтам исследований. Например, это отечественный проект «НОРА» (Национальный агрегатор открытых репозиториев), который предоставляет бесплатную электронную площадку для российских вузов и научных организаций, выпускающих периодические издания. Или зарубежные электронные площадки для поиска научных изданий по различным отраслям знаний—ORCID, ResearchGate, Mendeley, Google Scholar и другие.

С другой стороны, образовательная или научная организация рекомендует профессорско-преподавательскому составу и соискателям ученых степеней список научных периодических изданий, разработанный с учетом научных специальностей, по которым в организации ведется обучение и действует диссертационный совет.

Нельзя забывать и о научных периодических изданиях, отнесенных ко второй категории Перечня ВАК, которые могут находиться в открытом доступе в сети интернет для бесплатного ознакомления и последующего цитирования учеными.

Даже если научное периодическое издание, отнесенное к первой категории Перечня ВАК, находится в закрытом платном доступе, метаданные самих статей (данные об авторе и цитируемые им источники) могут быть открытыми, и, опираясь на них, ученый может сделать вывод о целесообразности покупки доступа к полному тексту. Или же, продолжив научный поиск, может найти похожие по теме статьи в открытом доступе.

Полностью решить проблему доступности научных изданий в электронном виде на данный момент не представляется возможным. Тем не менее, существует несколько решений, способствующих открытию доступа к публикациям и популяризации исследований.

Во-первых, это взаимный безвозмездный обмен между образовательными организациями издаваемой научной и учебной литературой в электронном виде для пополнения электронно-библиотечной системы вуза. Сотрудники библиотек образовательных организаций готовят ежеквартальные обзоры, дайджесты и тематические выставки, в которых информируют о новых поступлениях обучающихся и преподавателей.

Во-вторых, наличие подписки у библиотек образовательных организаций на коллекции научных периодических изданий в электронно-библиотечных системах и сторонних библиотеках (НЭБ «Elibrary.ru», «Лань», «Проспект», «Znanium» и др.).

В-третьих, налаживание научных связей в электронном виде между учеными для взаимного обмена публикациями на конференциях, очных или онлайн семинарах, или в социальных сетях.

В-четвертых, некоторые российские образовательные организации запускают международные конкурсы научных изданий, положение которых предполагает передачу в библиотечный фонд вуза на безвозмездной основе двух экземпляров научных изданий после завершения конкурсных процедур. В итоге участники конкурса получают признание (диплом лауреата) и популяризируют свои исследования, тогда как образовательная организация пополняет свой библиотечный фонд на безвозмездной основе и использует издания в образовательном процессе, в обновленных программах учебных дисциплин.

В-пятых, существуют сайты для выкладки авторами препринтов своих исследований (статей до рецензирования, отчетов НИР, предвари-

тельных результатов исследований) по гуманитарным и техническим наукам. Среди них можно выделить следующие: междисциплинарные архивы препринтов—https://arxiv.org/ и https://zenodo.org/; по психологии—https://psyarxiv.com/; по медицине—https://www.medrxiv.org/; по социальным наукам—https://socopen.org/; по биологии—https://www.biorxiv.org/; по криминологии—https://www.crimrxiv.com/; в области медиа-исследований—https://mediarxiv.org/ и другие.

В некоторых российских вузах также существуют репозитории для выкладки препринтов исследований. Например, в МГППУ на сайте журнала «Психологическая наука и образование» создан раздел «препринты»—https://psyjournals.ru/journals/pse/preprints, который содержит поступившие в редакцию статьи в формате «online first» и находящиеся в процессе публикации. То есть это статьи без нумерации страниц и без привязки к конкретному номеру выпуска, но с DOI и годом публикации. В НИУ ВШЭ создан каталог препринтов по тематическим сериям проводимых исследований (https://wp.hse.ru/prepid). В Институте прикладной математики имени М. В. Келдыша РАН выпускают в свободном доступе сериальное издание «Препринты ИПМ имени М. В. Келдыша» для оперативной публикации проводимых в институте исследований.

Любой онлайн-препринт допускает использование звука, видео, анимированных иллюстраций, перехода по ссылке к базам данных и пр. И не исключает последующей публикации в любом периодическом издании в текущем или доработанном виде на усмотрение авторского коллектива. В целом, препринт в сети интернет ускоряет коммуникацию между учеными и способствует развитию науки. Проверка препринта перед размещением на сайт осуществляется как модераторами сайта, так и искусственным интеллектом.

Таким образом, научное сообщество заинтересовано в ознакомлении с результатами исследований преимущественно в свободном доступе. И автор, чья статья находится в свободном доступе, быстрее получает отзыв и замечания, чем автор, чью статью нужно покупать для того, чтобы детально ознакомиться с результатами исследования. Коммерциализация публикаций, их перевод в закрытый платный доступ лишь замедляет научную коммуникацию. Рукописи, поступающие в научные периодические издания, отнесенные к первой категории Перечня ВАК, безусловно, проходят жесткий отбор перед публикацией, и когда они достигают читателя, можно быть уверенными, что результаты исследования корректны.

Приложение 1. Научные периодические издания по филологическим наукам, отнесенные к первой категории Перечня ВАК [6] и переаккредитованные по новым научным специальностям [7]

№ п/п	Наименование издания	Научные специальности (переаккредитация заштрихована)										Учредитель	Индексация	Доступ к архивам
		5.9.1.	5.9.2.	5.9.3.	5.9.4.	5.9.5.	5.9.6.	5.9.7.	5.9.8.	5.9.9.	5.12.3.			
1.	Studia Litterarum	■	■	■	■							РАН	Scopus; WoS (ESCI)	Открытый
2.	Terra Linguistica					■	■		■	■		Образовательная организация		Открытый
3.	Антропологический форум				■	■			■			РАН		Открытый
4.	Верхневолжский филологический вестник	■				■	■		■	■		Образовательная организация		Открытый
5.	Вестник Волгоградского государственного университета. Серия 2. Языкознание					■	■		■			Образовательная организация	WoS (ESCI)	Открытый
6.	Вестник древней истории							■				РАН	Scopus; WoS (ESCI)	**Платный, гибридный**
7.	Вестник Костромского государственного университета	■	■	■	■	■			■			Образовательная организация		Открытый
8.	Вестник Московского государственного областного университета								■			Образовательная организация		Открытый
9.	Вестник Нижегородского университета им. Н.И. Лобачевского					■			■			Образовательная организация		Открытый
10.	Вестник Новосибирского государственного университета. Серия: История, филология	■	■	■	■	■	■	■	■	■		Образовательная организация	Scopus	Открытый

[6] См.: Рекомендация ВАК Минобрнауки России от 26 октября 2022 года № 2-пл/1 «О новых критериях к соискателям ученых степеней кандидата наук, доктора наук, к членам диссертационных советов» [Электронный ресурс] // URL: https://vak.minobrnauki.gov.ru/uploader/loader?type=35&name=92246639002&f=13999 (дата обращения: 05.05.2023).

[7] См.: Перечень рецензируемых научных изданий, в которых должны быть опубликованы основные научные результаты диссертаций на соискание ученой степени кандидата наук, на соискание ученой степени доктора наук (по состоянию на 25.04.2023) [Электронный ресурс] // URL: https://vak.minobrnauki.gov.ru/uploader/loader?type=19&name=91107547002&f=17883 (дата обращения: 05.05.2023).

№ п/п	Наименование издания	Научные специальности (переаккредитация заштрихована)										Учредитель	Индексация	Доступ к архивам
		5.9.1.	5.9.2.	5.9.3.	5.9.4.	5.9.5.	5.9.6.	5.9.7.	5.9.8.	5.9.9.	5.12.3.			
11.	Вестник Пермского университета. Российская и зарубежная филология	▒	▒	▒	▒	▒	▒	▒	▒	▒	▒	Образовательная организация		Открытый
12.	Вестник РГГУ. Серия "Литературоведение. Языкознание. Культурология"			▒	▒			▒				Образовательная организация		Открытый
13.	Вестник Российского университета дружбы народов. Серия: Теория языка. Семиотика. Семантика								▒			Образовательная организация	Scopus	Открытый
14.	Вестник Самарского университета. История, педагогика, филология					▒	▒		▒	▒		Образовательная организация		Открытый
15.	Вестник Санкт-Петербургского университета. Язык и литература	▒	▒	▒	▒	▒	▒	▒	▒			Образовательная организация	Scopus; WoS (ESCI)	Открытый
16.	Вестник Северного (Арктического) федерального университета. Серия Гуманитарные и социальные науки					▒	▒		▒			Образовательная организация		Открытый
17.	Вестник Томского государственного педагогического университета	▒	▒			▒	▒		▒			Образовательная организация		Открытый
18.	Вестник Томского государственного университета	▒				▒			▒	▒	▒	Образовательная организация	WoS (ESCI)	Открытый
19.	Вестник Удмуртского университета. Серия История и филология	▒	▒	▒	▒	▒	▒		▒			Образовательная организация		Открытый
20.	Вестник Череповецкого государственного университета	▒		▒		▒	▒		▒			Образовательная организация		Открытый
21.	Вопросы когнитивной лингвистики	▒	▒	▒		▒	▒		▒	▒	▒	Образовательная организация	Scopus	**Платный**
22.	Вопросы ономастики							▒				РАН	Scopus; WoS (ESCI)	Открытый
23.	Гуманитарный вектор	▒							▒	▒		Образовательная организация		Открытый

№ п/п	Наименование издания	Научные специальности (переаккредитация заштрихована)										Учредитель	Индексация	Доступ к архивам
		5.9.1.	5.9.2.	5.9.3.	5.9.4.	5.9.5.	5.9.6.	5.9.7.	5.9.8.	5.9.9.	5.12.3.			
24.	Древняя Русь. Вопросы медиевистики	■		■		■						РАН	WoS (ESCI)	Открытый
25.	Жанры речи	■		■		■			■			Образовательная организация	Scopus	Открытый
26.	Известия Российского государственного педагогического университета им. А.И. Герцена					■	■		■			Образовательная организация		Открытый
27.	Известия Российской академии наук. Серия литературы и языка	■	■	■		■			■			РАН		**Платный, гибридный**
28.	Известия Самарского научного центра Российской академии наук. Социальные, гуманитарные, медико-биологические науки	■	■									РАН		Открытый
29.	Коммуникативные исследования	■		■		■			■	■		Образовательная организация		Открытый
30.	Наука и Школа	■	■							■		Образовательная организация		Открытый
31.	Наука о человеке: гуманитарные исследования	■	■	■	■	■				■		Образовательная организация		Открытый
32.	Научный диалог	■	■	■	■	■	■		■	■		Коммерческая организация	WoS (ESCI)	Открытый
33.	Преподаватель XXI век					■	■		■		■	Образовательная организация		Открытый
34.	Российский гуманитарный журнал			■								Коммерческая организация		Открытый
35.	Русистика					■						Образовательная организация	Scopus	Открытый
36.	Сибирский филологический журнал	■		■	■	■			■			РАН и образовательные организации	Scopus; WoS (ESCI)	Открытый
37.	СибСкрипт = SibScript	■		■		■	■		■			Образовательная организация		Открытый
38.	Томский журнал лингвистических и антропологических исследований.					■			■			Образовательная организация	WoS (ESCI)	Открытый

№ п/п	Наименование издания	Научные специальности (переаккредитация заштрихована)										Учредитель	Индексация	Доступ к архивам
		5.9.1.	5.9.2.	5.9.3.	5.9.4.	5.9.5.	5.9.6.	5.9.7.	5.9.8.	5.9.9.	5.12.3.			
39.	Уральский исторический вестник											РАН	Scopus	Открытый
40.	Ученые записки Казанского университета. Серия Гуманитарные науки											Образовательная организация		Открытый
41.	Филологические науки. Вопросы теории и практики											Коммерческая организация		Открытый
42.	Язык и культура											Образовательная организация	WoS (ESCI)	Открытый

Список источников:

1. Алимова, Н. К. Новая номенклатура специальностей, по которым присуждаются ученые степени // Научная периодика: проблемы и решения. — 2021. — Т. 10, № 1-2.

2. Крюкова, А. В. Организация научно-исследовательской работы: условия предоставления научной информации // Научные и технические библиотеки. — 2019. — № 10. — С. 68-76.

3. Куракова, Н. Г., Цветкова, Л. А. Категоризация Перечня ВАК и его место в национальной системе оценки эффективности исследований и разработок // Менеджер здравоохранения. — 2022. — № 10. — С. 4-13.

4. Степанов, В. К. Объективные факторы снижения роли библиотек в информационной деятельности // Научные и технические библиотеки. — 2023. — № 1. — С. 104-119.

Об авторе

Романова Светлана Андреевна — специалист отдела научного менеджмента и наукометрии Московского государственного лингвистического университета (Россия, Москва).
E-mail: s.a.romanova@linguanet.ru.

About the author

Svetlana A. Romanova — specialist of the Department of Scientific Management and Scientometrics Moscow State Linguistic University (Russia, Moscow).
E-mail: s.a.romanova@linguanet.ru.

УДК 004.8:316.28

ТРАНСФОРМАЦИЯ ПОНЯТИЯ КОММУНИКАТИВНОГО АКТА ПОД ВЛИЯНИЕМ ФАКТОРА ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Винников В. Ю.
Газета «Завтра» (Россия, Москва)
vinni-kov@yandex.ru

Аннотация

Статья посвящена проблемам трансформации термина «коммуникативный акт» и его структуры в теории коммуникации под влиянием фактора систем искусственного интеллекта. Выдвигается тезис о том, что структура коммуникативного акта с участием таких систем приобретает ряд особенностей, отличающих её от структуры «традиционных» коммуникативных актов, осуществляемых без участия искусственного интеллекта.

Ключевые слова

Искусственный интеллект, теория коммуникации, коммуникативный акт, структура коммуникативного акта, сигнальные системы.

Для цитирования: Винников В. Ю. Трансформация понятия коммуникативного акта под влиянием фактора искусственного интеллекта // Hi-Hume Journal.—2023.—№ 1 (1).—С. 145—149.

TRANSFORMATION OF THE CONCEPT OF A COMMUNICATIVE ACT UNDER THE INFLUENCE OF THE ARTIFICIAL INTELLIGENCE FACTOR

Vladimir Y. Vinnikov
Newspaper "Zavtra" (Moscow, Russia)
vinni-kov@yandex.ru

Abstract

The article is devoted to the problems of transformation of the term "communicative act" and its structure in the theory of communication under the influence of the factor of artificial intelligence systems. The thesis is put for-

ward that the structure of a communicative act involving such systems acquires a number of features that distinguish it from the structure of "traditional" communicative acts carried out without the participation of artificial intelligence.

Keywords
Artificial intelligence, communication theory, communicative act, structure of the communicative act, signaling systems.

For citation: Vinnikov V. Y. Transformation of the concept of a communicative act under the influence of the factor of artificial intelligence // Hi-Hume Journal.—2023.—№ 1 (1).—Pp. 145—149.

С начала XXI века всё более стремительное развитие информационных технологий, в том числе компьютерных (т.н. IT-революция), оказывает растущее комплексное влияние на все сферы бытия человеческой цивилизации, прежде всего—на её внутреннее коммуникативное пространство. Достижение этими технологиями качественно нового рубежа, обозначаемого в настоящее время термином «искусственный интеллект» (ИИ; англ. artificial intelligence, AI), создает множество проблем по всему спектру научного знания, включая общую теорию коммуникации, фундаментальные положения которой были сформированы ещё до начала IT-революции. То есть в данной сфере складывается ситуация, типологически сходная с переходом к релятивистской физике в начале XX века под влиянием таких обнаруженных в эксперименте и необъяснимых в рамках классической физики И. Ньютона факторов, как характер излучения абсолютно черного тела, радиоактивность и другие.

Данная ситуация дополнительно осложняется тем обстоятельством, что если «нижний порог» для понятия «искусственный интеллект» хотя бы приблизительно обозначен и признан (фальсифицирующий «тест Тьюринга», первое подтвержденное прохождение которого компьютерной программой в онлайн-режиме датируется 2014 годом), то относительно «верхнего порога» господствует полная неопределенность, что, в частности, приводит к таким событиям, как подготовленное по инициативе И. Маска и опубликованное в апреле 2023 года открытое письмо 1000 экспертов в сфере информационных технологий и искусственного интеллекта с призывом временно остановить разработку систем ИИ, более мощных, чем GPT-4, где были поставлены такие вопросы: «Должны ли мы развивать нечеловеческие умы, которые в конечном итоге могут превзойти нас численностью, перехитрить, сделать устаревшими

и заменить нас? Должны ли мы рисковать потерей контроля над нашей цивилизацией?» [7]—вопросы, аналогичные опасениям относительно атомного и термоядерного оружия.

Означает ли в данной связи развитие ИИ необходимость внесения необходимых изменений в общую теорию коммуникации, в частности —трансформации значения термина «коммуникативный акт», который в настоящее время всё чаще рассматривается как обозначение «эффективного синхронного и/или диахронного взаимодействия, цель которого состоит в передаче информации от одного субъекта к другому» [1, с. 69], т.е. в более общем значении, чем изначально предложенное Т.М. Ньюкомбом [8] «достижение общего отношения» (системной оценки, аттитюда) к тем или иным внешним факторам между акторами, входящими в коммуницирующую систему? При этом общепризнано, что коммуникативные акты свойственны не только человеческим сообществам, но и другим биологическим, от насекомых до высших млекопитающих [4], и даже экологическим, включающим в себя различные биологические виды, системам.

При этом следует отметить, что за акторами таких биологически коммуницирующих систем никогда ранее не признавался и в настоящее время не признается субъектный статус, соотносимый исключительно с человеком и человеческими сообществами. В то же время появление и развитие ИИ неизбежно ставит вопрос относительно критериев субъектности данного феномена, того комплекса системных параметров, по достижению которого «искусственный интеллект» должен будет рассматриваться уже как «искусственный субъект» и в этом статусе получать всё более полную коммуникативную, включая правовую, инклюзивность в рамках человеческих сообществ.

Но, пока этого не произошло, и статус субъекта за ИИ не признан и не подтвержден, данный тип участников коммуникативных актов следует рассматривать в качестве не субъектов, но акторов—так же, как это делается применительно к биологическим коммуницирующим системам. В пользу такого решения способен свидетельствовать и тот факт, что для ИИ, как и для биологических акторов, коммуникативные акты осуществляются преимущественно посредством сигналов, а не знаков как таковых. Иное дело, что информационная емкость таких сигналов способна превышать известный нам уровень аналогичного показателя для биологических сигналов на многие порядки.

В данном отношении, по аналогии с известным определением человеческой речи как «второй сигнальной системы», данным И.П. Павловым, можно говорить о формировании «третьей сигнальной системы»,

присущей системам ИИ и доступной для человека посредством «второй сигнальной системы» в виде сигналов устной и знаков письменной речи, но внутренне отличной от «второй сигнальной системы» и несводимой к ней. Поэтому вопрос о том, будет ли являться предполагаемая субъектность ИИ простой производной от социальной субъектности человека, пока остаётся принципиально открытым.

Все отмеченные факторы, как представляется, свидетельствуют о том, что структура коммуникативного акта с участием систем ИИ приобретает ряд особенностей, отличающих её от структуры «традиционных» коммуникативных актов без участия искусственного интеллекта, и эти особенности должны быть отражены в теории коммуникации—в том числе через трансформацию значения и, соответственно, спектра использования термина «коммуникативный акт», а также представлений о его структуре. В частности, речь может идти о преобразовании предложенной ещё Х. Ласуэллом [5] и широко используемой в настоящее время [2, 3, 6] классической линейной схемы, описывающей структуру коммуникативного акта как социальное антропное действие, в более многоуровневую (многомерную) и сетевого характера структуру.

То есть в общем виде одиночный акт информационной коммуникации, представляющий собой отправление, передачу и приём сигнала, может быть описан не по линейной схеме Х. Ласуэлла: «Who? → Says What? → In Which Channel? → To Whom? → With What Effect?», то есть «Кто? (передает сообщение)—Коммуникатор → Что? (передается)—Сообщение (текст) → Как? (осуществляется передача)—Канал → Кому? (направлено сообщение)—Аудитория → С каким эффектом?—Эффективность», а следующим образом (Схема 1). На данной схеме «семантическое поле» представляет собой множество (пространство) значений (смыслов), доступных акторам коммуникативного акта, как адресату, так и адресанту, вне и помимо ситуации самого коммуникативного акта, осуществляемого через сигнал коммуникации (вербальный и невербальный).

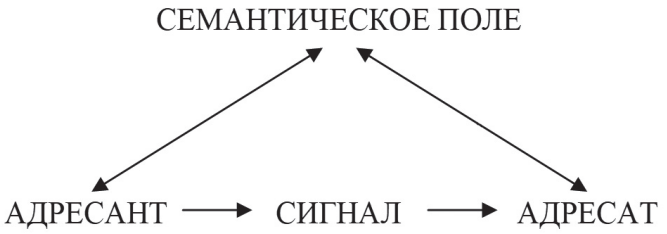

Схема 1. Акт информационной коммуникации

Список источников

1. Гавра Д. П. Основы теории коммуникации: учебник для вузов / Д. П. Гавра.—2-е изд., испр. и доп.—Москва : Издательство Юрайт, 2023.—231 с. [текст] [Электронный ресурс].—URL: https://urait.ru/bcode/511672 (дата обращения: 03.06.2023).

2. Benz A. Epistemic Perspectives and Communicative Acts.—Sec. Language Sciences.—2021.—Vol. 6.—20 p. [текст] [Электронный ресурс]—URL: https://doi.org/10.3389/fcomm.2021.612733

3. Casillas M., Hilbrink E. Communicative act development. In K. P. Schneider, & E. Ifantidou (Eds.), Developmental and Clinical Pragmatics.—Berlin: De Gruyter Mouton, 2020.—Pp. 61-88. [Электронный ресурс] URL: https://www.mpi.nl/publications/item3054065/communicative-act-development (дата обращения: 06.06.2023)

4. Fröhlich M., Bartolotta N., Fyns C., & oth. Multicomponent and multisensory communicative acts in orang-utans may serve different functions.—Commun. Biol. 4: 917 (2021). [Электронный ресурс] URL: https://www.nature.com/articles/s42003-021-02429-y (дата обращения: 07.06.2023)

5. Lasswell Harold D. The structure and function of communication in society. // The Communication of Ideas. N.Y.: Harper and Brothers,.—1948.

6. Murray Sarah E., Starr William B. The structure of communicative acts.—Springer Nature, Linguistics & Philosophy. Apr.2021. Vol. 44, Issue 2, p. 425-474 [текст] [Электронный ресурс]—URL: https://www.researchgate.net/publication/339937077_The_structure_of_communicative_acts (дата обращения: 02.06. 2023).

7. Musk E. & oth. Pause Giant AI Experiments: An Open Letter.—Future of Live.—2023, April 12. [текст] [Электронный ресурс]—URL: https://futureoflife.org/open-letter/pause-giant-ai-experiments (дата обращения: 07.06.2023).

8. Newcomb T. M. An approach to the study of communicative acts // Psychol. Rew.. —1953.— V. 60.—Pp. 293—304.

Об авторе

Винников Владимир Юрьевич— культуролог, заместитель главного редактора газеты «Завтра» (Россия, Москва).
E-mail: vinni-kov@yandex.ru.

About the authore

Vladimir Yu. Vinnikov — cultural scuentist, deputy editor-in-chief of the newspaper «Tomorrow» (Russia, Moscow).
E-mail: vinni-kov@yandex.ru.

ОБ АВТОРАХ

Бочкарев Олег Игоревич—студент 2-го курса (магистратура) Московского государственного лингвистического университета (Россия, Москва). E-mail: bo4karyow.oleg@yandex.ru.

Былевский Павел Геннадиевич—кандидат философских наук, доцент; Московский государственный лингвистический университет (Россия, Москва). E-mail: pr-911@yandex.ru.

Винников Владимир Юрьевич—культуролог, заместитель главного редактора газеты «Завтра». E-mail: vinni-kov@yandex.ru.

Гатауллин Сергей Тимурович—кандидат экономических наук, декан факультета «Цифровая экономика и массовые коммуникации» Московского технического университета связи и информатики (Россия, Москва), ведущий научный сотрудник Департамента информационной безопасности факультета информационных технологий и анализа больших данных Финансового университета при Правительстве РФ (Россия, Москва). E-mail: s.t.gataullin@mtuci.ru.

Гостев Александр Николаевич—доктор социологических наук, профессор, профессор кафедры информационной культуры цифровой трансформации, Московский государственный лингвистический университет (Россия, Москва). E-mail: Gostevan@inbox.ru.

Гришина Наталья Васильевна—кандидат технических наук, доцент, доцент кафедры информационной культуры цифровой трансформации Института информационных наук Московского государственного лингвистического университета (Россия, Москва). E-mail: grnat@rambler.ru.

Гусев Вадим Сергеевич—студент 4 курса (бакалавриат) Института информационных наук Московского государственного лингвистического университета (Россия, Москва). E-mail: bear.01@bk.ru.

Дробышев Артем Владиславович—студент 4-го курса (бакалавриат) Московского государственного лингвистического университета (Россия, Москва). E-mail: 2002temych2002@gmail.com.

Елин Владимир Михайлович—кандидат педагогических наук, доцент кафедры информационной культуры цифровой трансформации Института информационных наук Московского государственного лингвистического университета (Россия, Москва). E-mail: elin_vm@mail.ru.

Еремина-Драчева Юлия Максимовна—студент 2-го курса (магистратура) Российской академии народного хозяйства и государственной службы при президенте Российской Федерации, Москва (Россия, Москва). E-mail: yudracheva@gmail.com.

Карелова Оксана Леонидовна—доктор физико-математических наук, доцент, профессор кафедры международной информационной безопасности Московского государственного лингвистического университета, профессор кафедры прикладных информационных технологий Российской академии народного хозяйства и государственной службы при Президенте РФ (Россия, Москва). E-mail: okarelova@yandex.ru.

Кривошапка Полина Георгиевна—студент 4 курса (бакалавриат) Института информационных наук Московского государственного лингвистического университета (Россия, Москва). E-mail: polia.kr@yandex.ru.

Куковская Анна Владимировна—старший преподаватель кафедры лингвистики и профессиональной коммуникации в области информационных наук Института информационных наук Московского государственного лингвистического университета (Россия, Москва). E-mail: a.kukovskaya@linguanet.ru.

Мельникова Алина Александровна—студент 4 курса (бакалавриат) Московского государственного лингвистического университета (Россия, Москва). E-mail: pndlv12@gmail.com.

Пискунова Вероника Витальевна—студент 2 курса (магистратура) Московского государственного лингвистического университета (Россия, Москва); специалист по информационной безопасности ГК «Сател». E-mail: piskunova.nika@mail.ru.

Пелих Ярославна Владимировна—студент 2 курса (магистратура) Института информационных наук Московского государственного лингвистического университета, специалист ООО «ТТ-Трэвел» (Россия, Москва). E-mal: pelikh031@gmail.com.

Плешакова Екатерина Сергеевна—кандидат технических наук, доцент Департамента информационной безопасности факультета информационных технологий и анализа больших данных Финансового университета при Правительстве РФ (Россия, Москва). E-mail: espleshakova@fa.ru.

Романова Светлана Андреевна—специалист отдела научного менеджмента и наукометрии Московского государственного лингвистического университета (Россия, Москва). E-mail: s.a.romanova@linguanet.ru.

Садыхбекова Ляман Джамиль кызы—студент 4 курса (бакалавриат) Московского государственного лингвистического университета (Россия, Москва). E-mail: sdlyaman@yandex.ru.

Самойлов Вячеслав Евгеньевич—кандидат технических наук, и. о. заведующего кафедрой международной информационной безопасности Института информационных наук Московского государственного лингвистического университета (Россия, Москва), доцент кафедры системного анализа и информатики Российской академии народного хозяйства и государственной службы при Президенте РФ (Россия, Москва). E-mail: samoilov.1992@list.ru.

Федонин Александр Владимирович—студент 2 курса (магистратура) Института информационных наук; инженер-электроник отдела контрольно-пропускного режима, безопасности, антитеррористической и антикоррупционной деятельности Московского государственного лингвистического университета (Россия, Москва). E-mail: avladimir2021@yandex.ru.

Хлебцова Анастасия Петровна—студент 4 курса (бакалавриат) Института информационных наук Московского государственного лингвистического университета (Россия, Москва). E-mail: n.hleb@yandex.ru.

Цацкина Елена Петровна—кандидат педагогических наук, доцент ВАК, доцент кафедры международной информационной безопасности Института информационных наук Московского государственного лингвистического университета (Россия, Москва). E-mail: elena-tsatskina@yandex.ru.

Ястребов Евгений Сергеевич—студент 2 курса (магистратура) Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации (Россия, Москва). E-mail: ceo@brainy-lab.com.