ISSN 2518-1092

НАУЧНЫЙ РЕЗУЛЬТАТ

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

RESEARCH RESULT. INFORMATION TECHNOLOGY

8(2) 2023

16+

Сайт журнала:
rrinformation.ru
сетевой научный рецензируемый журнал
online scholarly peer-reviewed journal

НАУЧНЫЙ РЕЗУЛЬТАТ
RESEARCH RESULT

НАУЧНЫЙ РЕЗУЛЬТАТ. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ
RESEARCH RESULT. INFORMATION TECHNOLOGIES

Журнал зарегистрирован в Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор)
Свидетельство о регистрации средства массовой информации Эл. № ФС77-69101 от 14 марта 2017 г.

The journal has been registered at the Federal service for supervision of communications information technology and mass media (Roskomnadzor)
Mass media registration certificate El. № FS 77-69101 of March 14, 2017

Том 8, № 2. 2023

Volume 8, № 2. 2023

СЕТЕВОЙ НАУЧНО-ПРАКТИЧЕСКИЙ ЖУРНАЛ
Издается с 2016 г.
ISSN 2518-1092

ONLINESCHOLARLYPEER-REVIEWEDJOURNAL
First published online: 2016
ISSN 2518-1092

Учредитель: Федеральное государственное автономное образовательное учреждение высшего образования
«Белгородский государственный национальный исследовательский университет»
Издатель: НИУ «БелГУ». Адрес издателя: 308015 г. Белгород, ул. Победы, 85.
Журнал выходит 4 раза в год

Founder: Federal state autonomous educational establishment of higher education
«Belgorod State National Research University»
Publisher: Belgorod State National Research University
Address of publisher: 85 Pobeda St., Belgorod, 308015, Russia
Publication frequency: 4 /year

СОДЕРЖАНИЕ

CONTENTS

ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ

INFORMATION SYSTEM AND TECHNOLOGIES

АВТОМАТИЗАЦИЯ И УПРАВЛЕНИЕ

AUTOMATION AND CONTROL

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И ПРИНЯТИЕ РЕШЕНИЙ

ARTIFICIAL INTELLIGENCE AND DECISION MAKING

ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ
INFORMATION SYSTEM AND TECHNOLOGIES

УДК 004.934.5 **DOI: 10.18413/2518-1092-2022-8-2-0-1**

Джумаев А.Б.

О ПРОГРАММНЫХ СРЕДСТВАХ СИНТЕЗА РУССКОЙ РЕЧИ

ООО «ЛЕРУА МЕРЛЕН ВОСТОК», Осташковское шоссе, д.1, г. Мытищи, 141031 Россия

e-mail: art2371@yadex.ru

Аннотация
В современных информационных технологиях важное место занимают интерактивные методы ввода информации с последующим использованием обработанных данных. Голосовой ввод, управление жестами, захват движения, дополненная реальность, – данные средства в настоящее время широко используются в профессиональной деятельности и повседневной жизни человека. Синтез речи является частью речевых технологий, к которым также относятся распознавание речи, семантика речи и ее перевод. В настоящее время значительное количество исследователей занимаются изучением вопроса синтеза речи при создании новых программных продуктов. Поэтому оценка программных средств синтеза и сравнение их между собой является актуальной задачей. В данной работе проведён краткий анализ некоторых стационарных программных средств синтеза русской речи и дана оценка известным приложениям.
Ключевые слова: синтез речи; речевые технологии; системы синтеза речи; программные средства синтеза русской речи
Для цитирования: Джумаев А.Б. О программных средствах синтеза русской речи // Научный результат. Информационные технологии. – Т.8, №2, 2023. – С. 3-10. DOI: 10.18413/2518-1092-2022-8-2-0-1

Jumaev A.B.

ABOUT RUSSIAN SPEECH SYNTHESIS SOFTWARE

LLC «LEROY MERLIN VOSTOK», 1 Ostashkovskoe highway, Mytishchi, 141031 Russia

e-mail: art2371@yadex.ru

Abstract
In modern information technologies, an important place is occupied by interactive methods for entering information with the subsequent use of processed data. Voice input, gesture control, motion capture, augmented reality - these tools are currently widely used in professional activities and everyday life. Speech synthesis is a part of speech technologies, which also include speech recognition, speech semantics and its translation. Currently, a significant number of researchers are studying the issue of speech synthesis when creating new software products. Therefore, the evaluation of synthesis software tools and their comparison with each other is an urgent task. In this paper, a brief analysis of some stationary software tools for the synthesis of Russian speech is carried out and an assessment is made of known applications.
Keywords: speech synthesis; speech technologies; speech synthesis systems; Russian speech synthesis software
For citation: Jumaev A.B. About Russian speech synthesis software // Research result. Information technologies. – T. 8, №2, 2023. – P. 3-10. DOI: 10.18413/2518-1092-2022-8-2-0-1

ВВЕДЕНИЕ

Синтез речи на основе текстовых данных является актуальной задачей современности, так как синтезированная речь используется в различных сферах деятельности человека, к примеру, в банковских системах голосового самообслуживания, транспортных компаний, при проведении телефонных опросов и т.д.

В настоящее время известно несколько компаний и их программных продуктов, которые обладают поддержкой русского синтезированного языка – Microsoft Speech SDK (Microsoft), L&H (Lernout & Hauspie Speech Products) и Digalo (Elan Informatique) и другие.

Несмотря на то, что в мире существует масса разработок, проблема синтеза речи до сих пор не решена, так как качество синтезированной речи только в отдельных случаях можно считать удовлетворительной. Основными проблемами являются низкие показатели разборчивости, естественности и эмоциональности, которые приводят к ошибкам и сложности восприятия синтезированной речи [1, 2].

В рамках данной работы рассмотрены одни из наиболее распространённых стационарных сервисов синтеза речи, с позиций анализа их функциональных возможностей.

КЛАССИФИКАЦИЯ ПРОГРАММНЫХ СРЕДСТВ СИНТЕЗА РЕЧИ

Разработка первых русскоязычных синтезаторов началась в 2000-х года [3-11]. В настоящее время представлена масса разнообразных решений, как коммерческих, так и бесплатных. К глобальным отличиям существующих технологий можно отнести:

1. Количество поддерживаемых голосов;
2. Формат работы (отдельное приложение, вэб-версия, часть системы, интегрируемая библиотека);
3. Тип распространения (коммерческий, бесплатный);
4. Платформа использования.

В рамках исследования были отобраны и разбиты на 2 группы приложения, которые могут быть использованы для работы с персональным компьютером под управлением системой Windows и обладают поддержкой русского языка. Основной критерий разделения на группы является формат работы приложения.

К стационарным приложениям относятся:

1. «Говорилка»;
2. «Балаболка»;
3. «Vociebot»;
4. «NaturalReaders»;
5. «Robot Talk»;

К веб-приложениям относятся:

1. «2yxa»;
2. «Apihost»;
3. «Texttospeech»;
4. «TexttoSpeechRobot»;
5. «VoxWocker»;
6. «Ivona»;
7. «Acapela»;
8. «Microsoft Azure»;
9. «Yandex SpeechKit»;
10. «VoiceMaker»;
11. «OddCast».

В рамках данной работы проведён анализ группы стационарных приложений по синтезу русской речи.

СТАЦИОНАРНЫЕ ПРОГРАММНЫЕ СРЕДСТВА СИНТЕЗА РЕЧИ

Приложение **«Говорилка» –** стационарное приложение для семейства ОС Windows, основной задачей которого является озвучивание произвольного текста установленным голосом, интерфейс программы представлен на рисунке 1. Приложение основано на технологии конкатенативного синтеза. Данная технология использует конкатенацию предварительно записанных примеров человеческой речи в единую звуковую последовательность.

К основным возможностям программы относятся:

1. Запись генерируемой речи в звуковые файлы.
2. Регулировка скорости чтения и высоты тона голоса.
3. Система «слежения за речью», которая позволяет видеть озвучиваемый текст.
4. Пополняемые словари произношения с возможностью корректировки произношения.
5. Поддержка сторонних голосов.

Приложение «Говорилка» предлагает в стандартном исполнении 4 голоса (2 мужских и 2 женских), но количество голосов может быть расширено при помощи сторонних баз синтезированных голосов.

Преимущества данной программы совпадают с её основными возможностями, к минусам можно отнести:

1. низкое качество озвучиваемого текста,
2. низкая естественность речи,
3. большое количество ошибок произношения

Основные недостатки вызваны маленькой акустической базой голосов из-за чего «склейки» незнакомых слов происходят грубым образом, вызывая неестественное звучание.

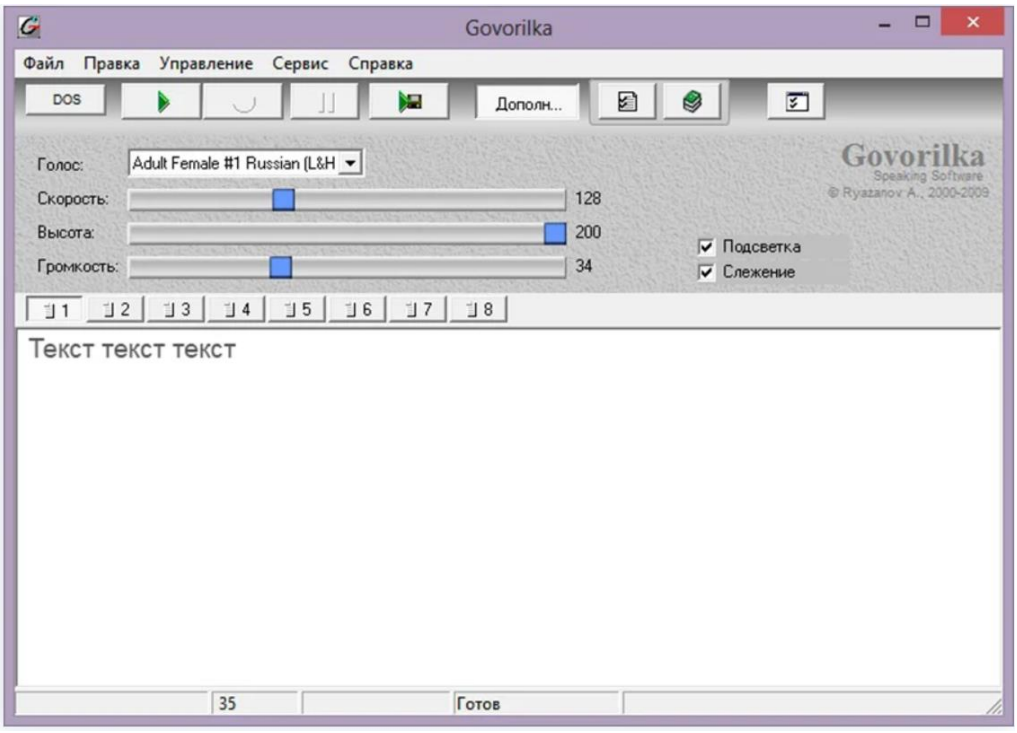

Рис. 1. Интерфейс программы «Говорилка»
Fig. 1. The interface of the «Govorilka» program

Приложение «**Балаболка»** – стационарное приложение для семейства ОС Windows, основной задачей которого является озвучивание произвольного текста, интерфейс программы представлен на рисунке 2. Данное приложение в своей основе так же, как и «Говорилка» использует метод синтеза речи на основе конкатенативного метода. Отличием данного речевого синтезатора от «Говорилки» является то, что для работы данной программы используется речевой

синтезатор операционной системы компьютера, то есть Microsoft Speech API системы Windows. К основным возможностям относятся:

1. Контроль воспроизведения речи
2. Возможность воспроизведения текста из буфера обмена
3. Озвучка набираемого текста
4. Экспорт речи в звуковые файлы

Недостатки данной программы совпадают с ранее выявленными для «Говорилки», дополнительно можно выделить:

1. Для замены голоса необходимы дополнительные плагины.
2. Отсутствует отдельный голос.

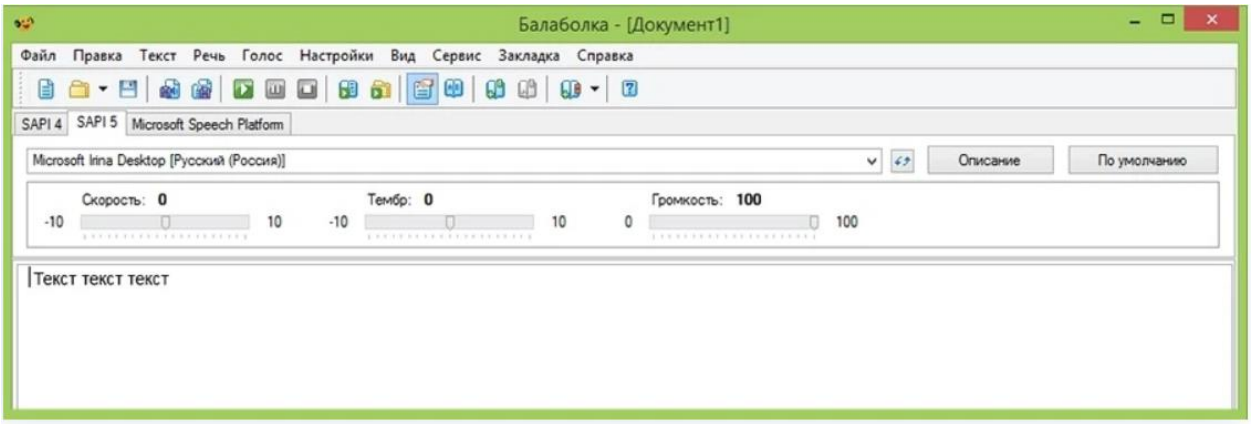

Рис. 2. Интерфейс программы «Балаболка»
Fig. 2. The interface of the «Balabolka» program

Приложение **«Voicebot» –** средство для программирования голосовых команд для управления системными службами ПК, интерфейс программы представлен на рисунке 3. В основе приложения, как и в предыдущих используется конкатенативный синтез. Данное средство не предназначено для целевого использования по озвучке текста и используется для узконаправленного использования по управлению персональным компьютером. Как и у сервиса «Балаболка» используется речевой синтезатор операционной системы компьютера. Данное программное обеспечение распространяется по платной подписке с бесплатным 30-дневным пробным периодом. «Voicebot» в процессе своей работы по заранее подготовленным командам производит распознавание речи пользователя и озвучку своих действий в рамках выполнения команд.

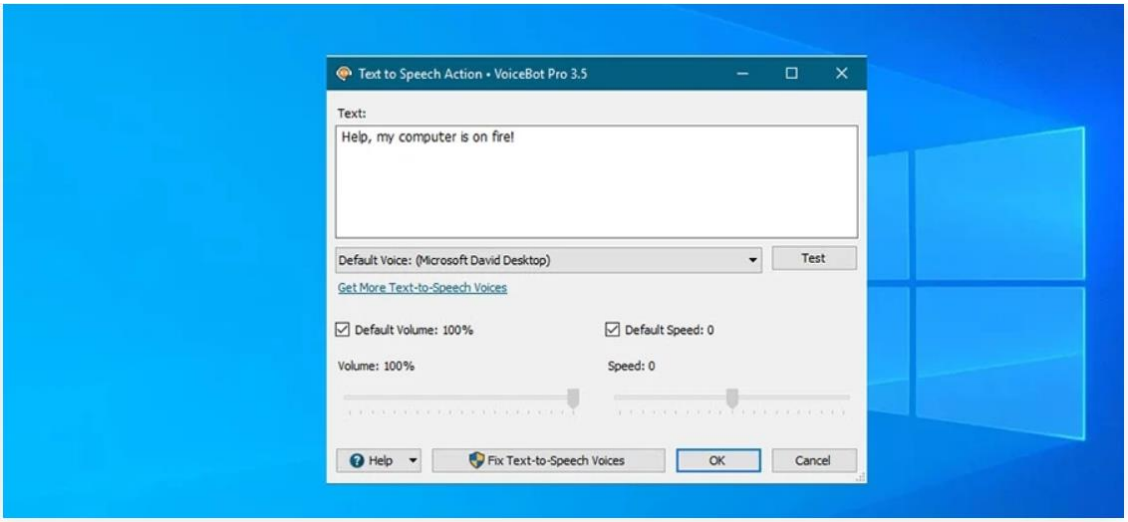

Рис. 3. Интерфейс программы «Voicebot»
Fig. 3. The interface of the « Voicebot » program

Приложение «**NaturalReaders**» **–** универсальное программное обеспечение, которое имеет, как стационарную версию приложения для персонального компьютера, так и веб-версию для генерации речи, интерфейс программы представлен на рисунке 4. В связи с ограничениями средство лишилось поддержки русского языка в обычном доступе, теперь для использования русского языка необходим пакет «Plus» в рамках платной подписки. Доступны 2 голоса (1 мужской и 1 женский), которые являются базовыми голосами для программного средства «Говорилка» и основаны на той же технологии. Так как «NaturalReaders» обладает двумя версиями приложения – стационарную и веб версии для них есть ряд отличающих особенностей:

1. Стационарная версия приложения может быть использована только на 1 компьютере, на котором была произведена установка средства;
2. При покупке лицензии для приложения будут разблокированы от 2 до 6 «премиальных» голосов, доступ к остальной библиотеке голосов можно получить за дополнительную плату в 40$ за каждый голос;
3. Для полноценной работы приложения не требуется подписка, что предполагает единоразовую оплату.

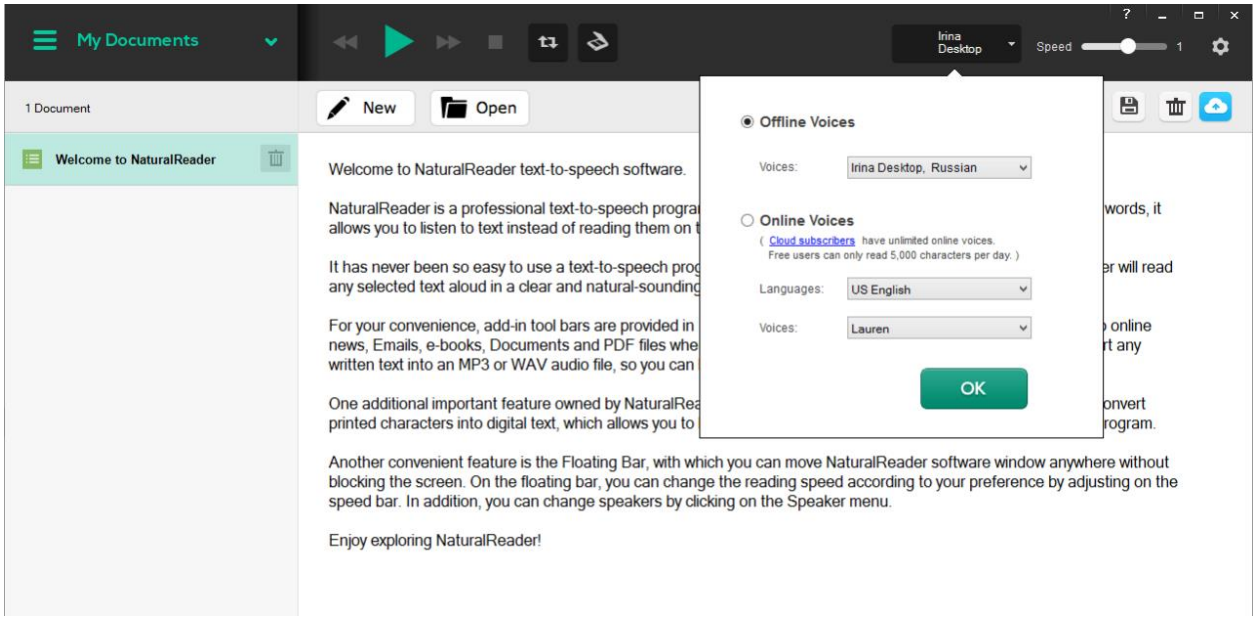

Рис. 4. Интерфейс программы «NaturalReaders»
Fig. 4. The interface of the «NaturalReaders» program

Приложение **«Robot Talk»** – бесплатное приложение (рис. 5) Windows Store, которое обладает 5 голосами (3 мужских и 2 женских), из которых 1 русский. Для синтеза речи используется та же технология, что и у предыдущих программных средств за исключением того, что Microsoft Speech API использует дополнительный модифицированный голос английской речи. Функциональные возможности приложения позволяют изменять тембр голоса и скорость речи. Так же присутствует возможность сохранения аудиофайлов. Недостатком данной программы является отсутствие русского интерфейса программы.

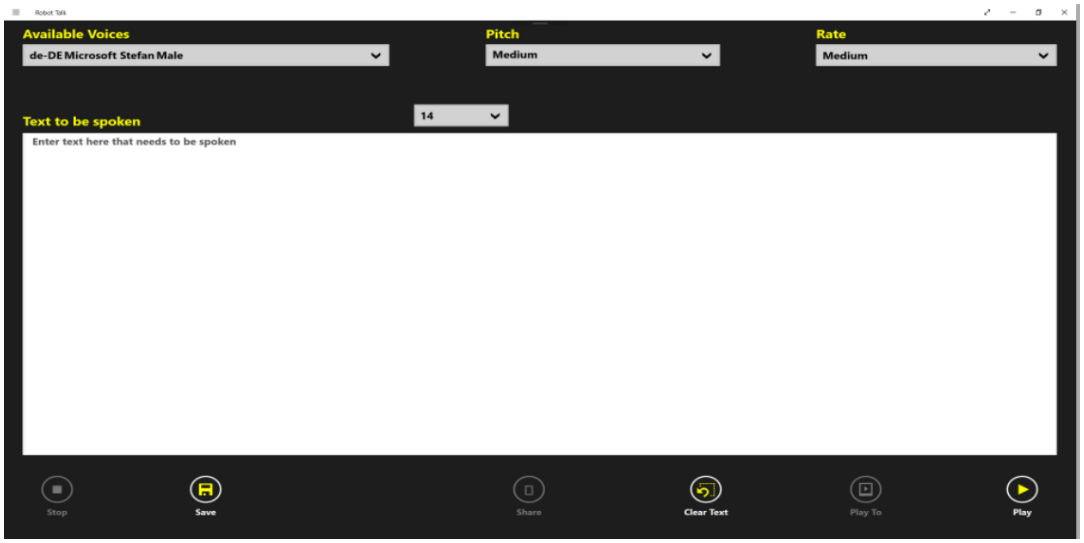

Рис. 5. Интерфейс программы «Robot Talk»
Fig. 5. The interface of the «Robot Talk» program

РЕЗУЛЬТАТЫ АНАЛИЗА СТАЦИОНАРНЫХ СРЕДСТВ

При наличии большого количества стационарных приложений их функционал не сильно отличается, а глобальные функции идентичны для всех программ. В зависимости от программы присутствует разброс по количеству голосов, но качество озвучивания у всех представленных аналогов находится на низком уровне и не может сравниться с естественной речью. Низкое качество синтезированной речи вызвано маленькой речевой базой и большим количеством ошибок при озвучивании. Малым исключением из списка является «Говорилка», так как она обладает функцией пополняемого словаря, что позволяет уменьшить количество ошибок синтеза речи в отличии от всех других представленных систем.

В таблице представлены сводные данные о стационарных средствах синтеза речи.

Таблица

Некоторые характеристики стационарных синтезаторов речи для русского языка

Table

Some characteristics of stationary speech synthesizers for the Russian language

Система синтеза	Доступные голоса	Преимущества	Недостатки	Комментарий
Говорилка	Николай Анна Digital Male voice Digital Female Voice	1. Большой выбор голосов; 2. Пополнение словаря произношений 3. Возможность установки сторонних голосов.	Низкое качество звучания	Оптимальное решение по функциональным возможностям
Балаболка	Встроенный в систему (Microsoft speech API)	1. Контроль воспроизведения речи; 2. Возможность воспроизведения текста из буфера обмена	1. Низкое качество звучания 2. Отсутствуют голоса, кроме предустановленных в систему	

Система синтеза	Доступные голоса	Преимущества	Недостатки	Комментарий
Vociebot	Встроенный в систему (Microsoft speech API)	Автоматизация задач управления ПК	Отсутствуют голоса, кроме предустановленных в систему	Узконаправленное ПО для автоматизации задач у правления ПК
NaturalReaders	Максим Ирина	Обладает, как стационарной версией, так и веб-версией	1. Высокая стоимость подписки 2. Ограничение на использование русскоязычных голосов	
Robot Talk	Встроенный в систему (Microsoft speech API)	-	1. Низкое качество звучания 2. 1 русскоязычный голос 3. Интерфейс программы на английском языке	Отсутствуют преимущества, т.к. модифицированный голос доступен только для английского языка

ЗАКЛЮЧЕНИЕ

В работе рассмотрены стационарные программные средства синтеза русской речи. При обзоре стационарных программных средств синтеза выявлена закономерность использования идентичных голосов, которые распространяются в рамках платного контента. Отличительной чертой является дополнительный функционал в виде эмоциональной окраски и регулировки тембра синтезированного голоса. Несмотря на то, что сервисов достаточно много, бесплатных решений доступно малое количество, при этом качество синтезированной речи – роботизированное в сравнении с естественной речью. Современной тенденцией является требование от ИТ-разработчиков создания облачных синтезаторов речи, а не стационарных, о чем свидетельствует значительное количество доступных средств синтеза речи в виде веб-приложений. Так как технологии синтеза речи находятся в процессе постоянного развития, то разработка новых синтезаторов русской речи доступна не только крупным ИТ-компаниям, но и частным разработчикам. Доступность данной технологии и спрос со стороны потребителя делает разработку новых программных средств синтеза речи актуальной задачей.

Список литературы

1. D.B.Keele, JR., Evaluation of Room Speech Transmission Index and Modulation Transfer Function by the Use of Time Delay Spectrometry, Techron, Div. Crown International, Inc., Elkhart, Indiana, 46517, USA.

2. A method for subjective performance assessment of the quality of speech voice output devices. ITU-T Recommendation P. 85. ITU-T, 1994.

3. Корольков В.А., Главатских И.А., Таланов А.О. Синтез естественной русской речи при помощи метода Unit Selection // Тр. XXXVI межд. Филолог. Конф. «Формальные методы анализа русской речи». Россия, 2008.

4. Джумаев А.Б. Синтезирование русской речи при помощи метода Unit Selection / VIII Международная научно-техническая конференция «Информационные технологии в науке, образовании и производстве», Белгород, 2020 г. – С. 43-46.

5. French N., Steinberg J. Factors Governing the Intelligibility of Speech Sounds // J.Acoust. 6 oc. Am. – 1947. – Vol. 19, No 1.

7. Fletcher H., Galt F. Perception of Speech and its Relation to Telephony // J. Acoust Soc. Am. – 1950. – Vol. 22, No 2.

7. Kryter K.D. Methods for the calculation and use of the articulation index // J. Acoust Soc. Am. – 1962. – Vol. 34. – P. 1689–1697.

8. ANSI S3.5-1997, American National Standard Methods for Calculation of the Speech Intelligibility Index – American National Standards Institute, New York. – 1997.

9. Беранек Л. Расчет речевых систем связи // Proceedings of the IRE. – 1947. – September. – P. 880-890.

10. Steeneken H.J.M., Houtgast T. RASTI: A Tool for Evaluating Auditoria // Bruel &Kjaer Technical Review No. 3 – 1985. – P.13-39.

11. Steeneken H.J.M., Houtgast T. RASTI: The Modulation Transfer Function in Room Acoustics // Bruel & Kjaer Technical Review No.3 – 1985. – P.1-12.

References

1. D.B.Keele, JR., Evaluation of Room Speech Transmission Index and Modulation Transfer Function by the Use of Time Delay Spectrometry, Techron, Div. Crown International, Inc., Elkhart, Indiana, 46517, USA.

2. A method for subjective performance assessment of the quality of speech voice output devices. ITU-T Recommendation P. 85. ITU-T, 1994.

3. Korolkov V.A., Glavatskikh I.A., Talanov A.O. Synthesis of natural Russian speech using the Unit Selection method // Tr. XXXVI Int. Philologist. Conf. "Formal Methods for the Analysis of Russian Speech". Russia, 2008.

4. Dzhumaev A.B. Synthesizing Russian speech using the Unit Selection method / VIII International Scientific and Technical Conference "Information Technologies in Science, Education and Production", Belgorod, 2020 – P. 43-46.

5. French N., Steinberg J. Factors Governing the Intelligibility of Speech Sounds // J.Acoust. 6 oc. Am. – 1947. – Vol. 19, No 1.

7. Fletcher H., Galt F. Perception of Speech and its Relation to Telephony // J. Acoust Soc. Am. – 1950. – Vol. 22, No 2.

7. Kryter K.D. Methods for the calculation and use of the articulation index // J. Acoust Soc. Am. – 1962. – Vol. 34. – P. 1689–1697.

8. ANSI S3.5-1997, American National Standard Methods for Calculation of the Speech Intelligibility Index – American National Standards Institute, New York. – 1997.

9. Beranek L. Calculation of speech communication systems // Proceedings of the IRE. – 1947. – September. – P. 880-890.

10. Steeneken H.J.M., Houtgast T. RASTI: A Tool for Evaluating Auditoria // Bruel &Kjaer Technical Review No. 3 – 1985. – P.13-39.

11. Steeneken H.J.M., Houtgast T. RASTI: The Modulation Transfer Function in Room Acoustics // Bruel & Kjaer Technical Review No. 3 – 1985. – P.1-12.

Джумаев Артём Бахтиёрович, аналитик ИТ-процессов отдела поддержки пользователей ООО «Леруа Мерлен Восток»

Jumaev Artem Bakhtierovich, IT process analyst of the User Support Department of Leroy Merlin Vostok LLC

УДК 004.056 **DOI: 10.18413/2518-1092-2022-8-2-0-2**

Кузьминых Е.С.
Маслова М.А.

АНАЛИЗ РОСТА КИБЕРАТАК И РЫНКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РФ

Севастопольский государственный университет, ул. Университетская, д. 33, г. Севастополь, 299053, Россия

e-mail: egor2014ru@mail.ru, mashechka-81@mail.ru

Аннотация
Сфера IT прогрессирует без остановки, из-за чего сотрудникам информационной безопасности приходится регулярно прогрессировать вместе со всеми обновлениями программного обеспечения для максимальной результативности обеспечения безопасности компании, в которой они работают. Для этого компаниям необходимо нанимать квалифицированного сотрудника информационной безопасности, который будет обучать персонал «правильно» обращаться с компьютером, будет регулярно обновлять программное обеспечение, устанавливать новое и сможет в режиме реального времени противостоять атакам злоумышленников. В 2022 году на российский сегмент обрушились нападения зарубежных хакеров, что привело к большим проблемам для всех отраслей страны. Компаниям и государственным структурам пришлось противостоять постоянным атакам. В настоящее время происходит переход на отечественное ПО, что облегчает ситуацию. Также в 2022-2023 годах было выделено большое количество средств на разработку нового ПО и борьбу со злоумышленниками. В данной статье были рассмотрены некоторые виды атак на компании, самая актуальная, 0-day, какая информация больше интересует злоумышленников, какие отрасли подверглись атакам и каким образом. Как все эти изменения повиляли на российский рынок ИБ и прогнозы на будущее.
Ключевые слова: кибератаки; атаки; хакеры; злоумышленники; атака нулевого дня; 0-day; отечественное ПО; рынок; информационная безопасность; ИБ; антивирусы; безопасность; российские сегменты; бюджет; бюджет ИБ; импортозамещение
Для цитирования: Кузьминых Е.С., Маслова М.А. Анализ роста кибератак и рынка информационной безопасности РФ // Научный результат. Информационные технологии. – Т.8, №2, 2023. – С. 11-18. DOI: 10.18413/2518-1092-2022-8-2-0-2

Kuzminykh E.S.
Maslova M.A.

ANALYSIS OF THE GROWTH OF CYBERATTACKS OF THE INFORMATION SECURITY MARKET OF THE RUSSIAN FEDERATION

Sevastopol state University, 33 Universitetskaya St., Sevastopol, 299053, Russia

e-mail: egor2014ru@mail.ru, mashechka-81@mail.ru

Abstract
The IT sphere is progressing without stopping, which is why information security employees have to regularly progress along with all software updates to maximize the effectiveness of ensuring the security of the company in which they work. To do this, companies need to hire a qualified information security officer who will train staff to "properly" use a computer, will regularly update software, install new ones and will be able to withstand attacks by intruders in real time. In 2022, the Russian segment was attacked by foreign hackers, which led to big problems for all sectors of the country. Companies and even government agencies had to resist constant attacks. Currently, there is a transition to domestic software, which makes the situation easier. Also, in 2022-2023, a large amount of funds was allocated for the development of new software and the fight against intruders. In this article, some types of attacks on companies were considered, the most relevant, 0-day, which information is more interested in attackers, which

industries were attacked and how. How all these changes affected the Russian information security market and forecasts for the future.
Keywords: cyber-attacks; attacks; hackers; intruders; zero-day attack; 0-day; domestic software; market; information security; IB; antiviruses; security; Russian segments; budget; IB budget; import substitution
For citation: Kuzminykh E.S., Maslova M.A. Analysis of the growth of cyberattacks of the information security market of the Russian Federation. – Т.8, №2, 2023. – P. 11-18. DOI: 10.18413/2518-1092-2022-8-2-0-2

ВВЕДЕНИЕ

В век развития информационных технологий сфера IT развивается достаточно быстро, появляются новые технологии, программное обеспечение и постоянное обновление ранее созданного, что приводит к появлению новых проблем и ошибок в работе той, или иной системы. На фоне этого актуален вопрос, как же защищать все эти технологии, чтобы хоть немного обезопасить себя, или компанию от злоумышленников. Данный вопрос решает сфера Информационной безопасности, сотрудники которой регулярно развивают себя, следят за новинками, обновлениями и создающимися новыми угрозами со стороны злоумышленников.

В последние годы идёт развитие отечественного программного обеспечения, заменяют иностранное ПО на российское и поддерживают любых разработчиков в грамотных идеях по разработке. Благодаря чему появляется всё больше самостоятельных и новых компаний, которые развивают новое ПО. Сотрудники IT получают множество бонусов от правительства и чувствуют себя как «рыба в воде», благодаря чему рынок информационной безопасности начал расти с каждым годом.

ОСНОВНАЯ ЧАСТЬ

Существует множество проблем информационной безопасности, как и различное ПО для атак на компании. В основном злоумышленники пользуются уязвимостью нулевого дня. 0-day — обозначает, что существуют уязвимости, для которых не нашли способа устранения, или вредоносное ПО, против которых не разработали защитные методы. Сложно предсказать, где именно в коде будет ошибка, из-за которой злоумышленник сможет проникнуть в систему. В настоящее время многие создатели вирусов фокусируются именно на неизвестных уязвимостях, т.к. компания может быть не готова к такой атаке и даже не знать про проблему, через которую проберётся злоумышленник [1, 2].

Для нахождения уязвимостей создатели вирусов используют различные методы, например:

- реверс-инжиниринг и поиск ошибок в алгоритме работы ПО;
- дизассемблирование кода и поиск ошибок в самом коде ПО;
- фаззинг-тестирование — тестирование программного обеспечения, суть заключается в обработке программой большого количества информации, которая изначально содержит неверные параметры [3].

Классические антивирусы не способны обнаружить такую атаку, поэтому их защита для компаний незначительна. Для эффективной защиты от атак 0-day используют проактивные технологии защиты. Они эффективно обеспечивают защиту от новых, известных, атак и вирусов. Но всё равно абсолютную защиту данный метод предоставить не может, т.к. нельзя защититься от всего, тем более от новой атаки.

Проактивная защита — это комплекс организационных и технических мер, которые позволяют расширить понятие защищённости и повысить реакцию web-приложений на новые угрозы и нападения [4].

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ И ИХ ОБСУЖДЕНИЕ

Не стоит забывать про обычные вирусы и атаки, которые постоянно мешают компаниям нормально функционировать. В 2022 году на российские компании было совершено в два раза больше атак, чем в прошлом году, примерно 900 тысяч хакерских атак. Атаки от обычных активистов, которые не преследуют коммерческие цели, значительно снизились, а именно DDoS-атаки на web-ресурсы. 2022 год был очень опасен для компаний, никогда не было таких активных и хаотичных атак на разные ресурсы Российской Федерации, которые к концу года перешли в более целенаправленные и конкретные атаки. Значительно выросли сетевые атаки. Сканирование сети происходит автоматизированными инструментами, для компрометации учётных записей пользователей и разведки сети компаний. Хоть и таких инцидентов мало, но это означает, что такая информация более интересна для злоумышленников.

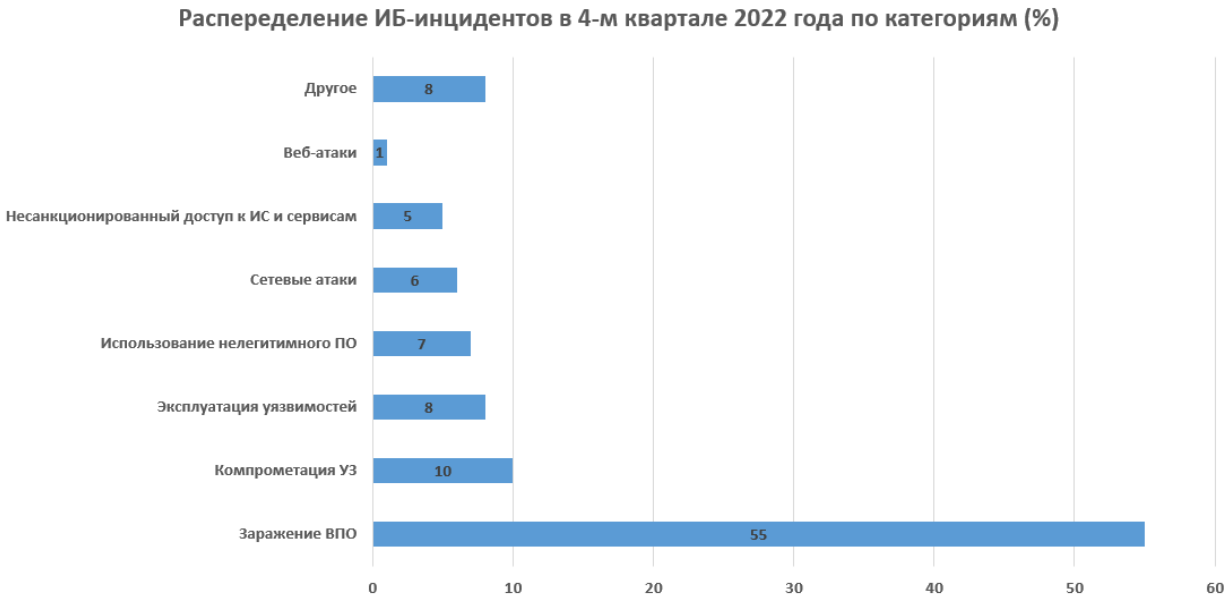

Рис. 1. Категории атак на российские компании [5]
Fig. 1. Categories of attacks on Russian companies [5]

В 62% случаев хакеры использовали вредоносное ПО, в основном шифровальщики, направленные на кражу конфиденциальных данных и получение выкупа. Но всё же, больший процент атак совершён на частные лица, ведь у не грамотного пользователя легче украсть данные, чем у целой компании.

В 2022 году увеличились атаки на российские сегменты и все ключевые отрасли экономики. Можно выделить следующие позиции:

– государственный сектор — был целью №1, было зафиксировано 403 атаки, что на 25% больше, чем в прошлом году. Государственный сектор был лакомым кусочком для преступных организаций, желающих похитить секретную информацию и навредить стране;

– промышленность — злоумышленники хотели остановить работу отраслевой промышленности, или замедлить выпуск продукции. Было зафиксировано 223 атаки, что на 7% больше в отличии от прошлого года. В основном использовались методы социальной инженерии, в некоторых случаях компрометация программного обеспечения в компаниях;

– медицина — уже несколько лет занимает 3-е место по атакуемым отраслям, занимает лидирующую позицию по утечке данных. Более чем в 80% случаев происходит утечка конфиденциальных данных клиентов. В системах медучреждений содержатся колоссальный объем данных, преступники могут получить такие конфиденциальные данные как: историю

болезни, ФИО, информацию о состоянии здоровья, номер телефона, реквизиты счетов, номеров карт, адрес прописки, или электронной почты, дату рождения и любую другую медицинскую информацию.

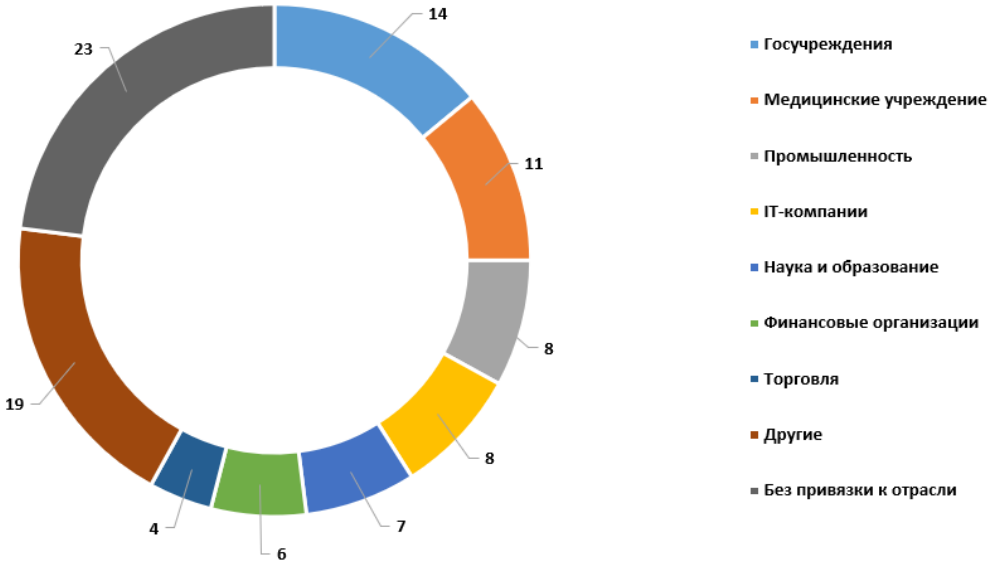

Рис. 2. Категории жертв среди организаций
Fig. 2. Categories of victims among organizations

– финансовый сектор — по сравнению с прошлым годом атаки на данный сектор снизились на 7%. Компании более подготовлены к атакам, но это не гарантирует хорошей защищённости. Positive Technologies провели исследование, в ходе которого в 86% случаев получили доступ к локальной сети. Помимо этого, было выяснено, что в режиме реального времени можно проникнуть глубже в сеть даже не опытному злоумышленнику. В ходе проверки все эксперты смогли получить полный доступ к инфраструктуре компании и показали, что будет, если злоумышленник попадёт в сеть [6 - 8];

– IT-компании — процент атак снизился, однако 6% атак принадлежат данному сектору. IT-компании более готовы к атакам и в большинстве таких компаниях есть квалифицированный сотрудник информационной безопасности, который обеспечивает защиту сети и способен потягаться со злоумышленником в режиме реального времени. Как и во всех компаниях, в большинстве случаев используется метод социальной инженерии, ведь так гораздо легче проникнуть в сеть компании, приложив минимум усилий;

– наука и образование — количество атак в отличии от 2021 года не изменилось, злоумышленников всё так же интересует конфиденциальная информация, преимущественно персональные данные клиентов и сотрудников. Каждая вторая атака была совершена шифровальщиками, целью данной атаки было получение выкупа от организации за украденную информацию. Также подбирали пароли от учётных записей и пользовались скомпрометированными данными;

– пользователи — количество атак на обычных пользователей выросло на 44%, что привело к масштабным утечкам данных. 17% от общего числа атак пришлось на пользователей. Способы атак такие же, как и в прошлых отраслях.

Из-за роста атак бюджет информационной безопасности увеличили у государственных структур на 26%, средства пошли на продление лицензий, закупку нового железа и ПО. Объём рынка информационной безопасности в 2021 году достиг 98,6 млрд. рублей, что означает рост на 8%, в 2022 году вырос на 10-20% [10]. В начале 2022 года компании думали, что рынок упадёт на 20%, из-за ухода западных производителей, но из-за активных атак на инфраструктуру Российской Федерации многие компании столкнулись с проблемами, на которые нужно было реагировать.

Заказчики стали чаще обращаться к экспертам, что привело к росту рынка и резкому увеличению спроса на сервисы ИБ. Это вызвано некоторыми причинами:

– выросли продажи firewall'ов примерно в 3 раза и во столько же раз анализаторы кода на поиск уязвимостей;

– сфера ИБ более готова к отечественному импортозамещению, чем вся остальная IT-сфера, часть бюджетных средств заказчиков были перенаправлены на средства защиты, т.к. срочно требовались новые инвестиции для проектов;

– государство стало требовать от кибербезопасности результата — отсутствия взломов и утечек информации, а не как раньше, сертификации объектов, что заставило «расшевелиться» сфере ИБ.

В 2023 году рынок ИБ закрепится на отечественном производителе, если в 2022 ещё были некоторые закупки западных разработчиков, то в будущем это будет сводиться к нулю. В 250-м указе президента было указано, что после 1 января 2025 года все компании обязаны использовать средства защиты информации только отечественного производителя. Это приведёт к появлению новых средств и серьёзной борьбе компаний-гигантов, кто первый успеет, тот и получит большую выгоду и преимущества.

К 2025 году прогнозируют рост рынка на 43,8 млрд. рублей, что в общей сумме будет равно 131,8 млрд. рублей. В 2022 году множество зарубежных производителей ушли из страны, что привело к некоторым проблемам. Но где есть минусы, там есть и плюсы. Правительству пришлось задуматься о замене таких производителей, что привело к идее отечественного импорт замещения. С 2025 года отечественным компаниям будет запрещено использовать иностранное ПО, поэтому большинство проектов развиваются довольно быстро. Уже в 2023 и 2024 годах начнут внедрение некоторых отечественных ПО на предприятиях и начнут их тестирование, а к 2025 и 2027 по прогнозу закончат все проекты по импортозамещению [9, 11- 13].

ЗАКЛЮЧЕНИЕ

Кибербезопасность очень важна в любой области, будь то бизнес-сфера, медицина, образование, или государственные учреждения. На основе проведённого исследования становится понятно, что злоумышленники никогда не сидят на месте, регулярно следят за всеми обновлениями и появлением новых технологий, постоянно ищут способы проникнуть через защиту, чтобы взломать ту, или иную компанию. Поэтому не стоит недооценивать своих «врагов», необходимо качественно защищать себя и свою компанию. Для этого необходимо обучаться грамотному использованию ПК и существующих программ для защиты от угроз и уязвимостей, также обучать персонал своих компаний проводя постоянные курсы повышения квалификации, а также при необходимости переквалификации. Ни в коем случае нельзя экономить на бюджете направленным на обеспечение безопасности компании, ведь лучше потратить лишние средства на защиту, чем потерять всё из-за экономии.

Конечно, чаще всего нападения совершаются на частные лица, ведь украсть их данные гораздо легче, потому что они менее подготовлены к нападениям, но и большинство компаний тоже страдает от нападений. Уже довольно скоро появятся альтернативные отечественные ПО, которыми начнут пользоваться компании для повседневной деятельности и защиты своих сетей и т.д. Такое ПО будет легче настраивать, модернизировать, т.к. оно разработано нашими программистами, что принесёт свои плоды.

Список литературы

1. Авраменко В.С., Бобрешов-Шишов Д.И., Маликов А.В. Способ выявления уязвимостей «нулевого дня» на основе анализа поведения эксплойтов // Проблемы технического обеспечения войск в современных условиях. – 2018. – С. 45-48.

2. Гладушенко С.Г., Искольный Б.Б. Оценка вероятности компьютерных атак нулевого дня // REDS: Телекоммуникационные устройства и системы. – 2017. – Т. 7. – №. 4. – С. 481-483.

3. Атака нулевого дня информации [Электронный ресурс]. URL: https://dzen.ru/a/W-b33EE2PACqYwQf
4. Проактивная защита [Электронный ресурс]. URL: https://helpdesk.bitrix24.ru/open/9160201/
5. Число кибератак в России и в мире [Электронный ресурс]. URL: https://www.tadviser.ru/index.php/Статья:Число_кибератак_в_России_и_в_мире
6. Positive Technologies: что принес ушедший год и каких вызовов кибербезопасности ждать в 2023-м [Электронный ресурс]. URL: https://www.ptsecurity.com/ru-ru/about/news/positive-technologies-chto-prines-ushedshij-god-i-kakih-vyzovov-kiberbezopasnosti-zhdat-v-2023-m/
7. Маслова М.А. Риски IT-инфраструктуры и методы их решения // Научный результат. Информационные технологии. – Т.7, №4, 2022. С. 34-40. DOI: 10.18413/2518-1092-2022-7-4-0-4.
8. Российское программное обеспечение (Отечественное ПО) [Электронный ресурс]. URL: https://www.tadviser.ru/index.php/Статья:Российское_программное_обеспечение_(Отечественное_ПО)
9. Переход на отечественное ПО ускорится в 2023 году [Электронный ресурс]. URL: https://rg.ru/2023/02/02/perehod-na-otechestvennoe-po-uskoritsia-v-2023-godu.html
10. Информационная безопасность (рынок России) [Электронный ресурс]. URL: https://www.tadviser.ru/index.php/Статья:Информационная_безопасность_(рынок_России)
11. Омельченко В.И., Исаев М.Ю. Использование планшетных компьютеров с отечественным программным обеспечением при проведении учебных занятий // Информационные технологии: актуальные проблемы подготовки специалистов с учетом реализации требований ФГОС. – 2021. – С. 354-357.
12. Голубев О.Б., Попова Е.Ю. Использование отечественного программного обеспечения в учебном процессе // Современные проблемы и перспективы обучения математике, физике, информатике в школе и вузе. – 2020. – С. 168-172.
13. Маслова М.А., Смирнов Н.С. Программная реализация оценки рисков информационной безопасности // Современные проблемы радиоэлектроники и телекоммуникаций. – 2022. – № 5. – С. 203.

References

1. Avramenko V.S., Bobreshov-Shishov D.I., Malikov A.V. A method for identifying zero-day vulnerabilities based on the analysis of exploits behavior // Problems of technical support of troops in modern conditions. – 2018. – pp. 45-48.
2. Gladushenko S.G., Iskolny B.B. Assessment of the probability of zero-day computer attacks // REDS: Telecommunication devices and systems. – 2017. – Vol. 7. – No. 4. – pp. 481-483.
3. Zero-day information attack [Electronic resource]. URL: https://dzen.ru/a/W-b33EE2PACqYwQf.
4. Proactive protection [Electronic resource]. URL: https://helpdesk.bitrix24.ru/open/9160201/.
5. The number of cyber-attacks in Russia and in the world [Electronic resource]. URL: https://www.tadviser.ru/index.php/Статья:Number of cyberattacks in_Russia_and_world.
6. Positive Technologies: what the past year has brought and what challenges to cybersecurity to expect in 2023 [Electronic resource]. URL: https://www.ptsecurity.com/ru-ru/about/news/positive-technologies-chto-prines-ushedshij-god-i-kakih-vyzovov-kiberbezopasnosti-zhdat-v-2023-m/.
7. Maslova M.A. IT infrastructure risks and methods for their solution // Research result. Information technologies. – T.7, №4, 2022. – P. 34-40. DOI: 10.18413/2518-1092-2022-7-4-0-4.
8. Russian software (Domestic software) [Electronic resource]. URL: https://www.tadviser.ru/index.php/Статья:Russian Software Support_(Domestic_BY).
9. The transition to domestic software will accelerate in 2023 [Electronic resource]. URL: https://rg.ru/2023/02/02/perehod-na-otechestvennoe-po-uskoritsia-v-2023-godu.html.
10. Information security (Russian market) [Electronic resource]. URL: https://www.tadviser.ru/index.php/Статья:Information Security (Market_Russia).
11. Omelchenko V.I., Isaev M.Yu. The use of tablet computers with domestic software during training sessions // Information technologies: actual problems of training specialists taking into account the implementation of the requirements of the Federal State Educational Standard. – 2021. – pp. 354-357.
12. Golubev O.B., Popova E.Yu. The use of domestic software in the educational process // Modern problems and prospects of teaching mathematics, physics, computer science at school and university. – 2020. – pp. 168-172.

13. Maslova M.A., Smirnov N.S. Software implementation of information security risk assessment Modern problems of radio electronics and telecommunications. – 2022. – № 5. – P. 203.

Кузьминых Егор Сергеевич, студент третьего курса кафедры Информационная безопасность Института информационных технологий
Маслова Мария Александровна, старший преподаватель кафедры Информационная безопасность Института информационных технологий

Kuzminykh Egor Sergeevich, Third-year Student of the Department Information security, Institute of Information Technologies
Maslova Maria Alexandrovna, Senior Lecturer of the Department Information security Institute of Information Technologies

УДК 004 **DOI: 10.18413/2518-1092-2022-8-2-0-3**

Дмитриева Т.И.
Абрамова О.Ф.

ИССЛЕДОВАНИЕ И АНАЛИЗ ПРОБЛЕМ РАЗВИТИЯ КРЕАТИВНОГО МЫШЛЕНИЯ В ОБЛАСТИ ГРАФИЧЕСКОГО ДИЗАЙНА У СОВРЕМЕННОЙ МОЛОДЕЖИ

Волжский политехнический институт (филиал) ФГБОУ ВО «Волгоградский государственный технический университет», ул. Энгельса, д. 42а, г. Волжский, Волгоградская область, 404121, Россия
e-mail: mrsanytanittt@gmail.com, oxabra@yandex.ru

Аннотация
В данной статье поднимается проблема развития креативного мышления современной молодежи в области графического дизайна, а также исследуются проблемы и решения в области дистанционного образования. Как показывают исследования, использование цифровых технологий в учебном процессе сильно меняет роль педагога. С другой стороны, современные обучающиеся ожидают повышения интерактивности учебного процесса, использования инновационных цифровых решений и возможности проявить свою креативность. В статье рассмотрены понятия геймификации образования и креативного мышления применительно к области обучения графическому дизайну. Геймификация в образовании – это использование игрового процесса как метода обучения, который позволяет улучшить вовлеченность учеников и повысить их мотивацию к обучению. С другой стороны, развитие креативного мышления - способности находить необычные и эффективные решения проблем – так же необычайно важно для будущих дизайнеров и художников. В статье рассмотрены способы развития креативного мышление в процессе обучения графическому дизайну, определены проблемы онлайн-образования в целом и обучения графическому дизайну в частности. В заключительной части статьи приведены модели функциональных требований для реализации веб-системы для обучения графическому дизайну и результаты исследования потенциальных пользователей такой системы.

Ключевые слова: онлайн-образование; креативное мышление; геймификация образования; графический дизайн; обучение
Для цитирования: Дмитриева Т.И., Абрамова О.Ф. Исследование и анализ проблем развития креативного мышления в области графического дизайна у современной молодежи // Научный результат. Информационные технологии. – Т.8, №2, 2023 – С. 18-25. DOI: 10.18413/2518-1092-2022-8-2-0-3

Dmitrieva T.I.
Abramova O.F.

RESEARCH AND ANALYSIS OF THE PROBLEMS OF DEVELOPING CREATIVE THINKING IN THE FIELD OF GRAPHIC DESIGN AMONG MODERN YOUTH

Volzhsky Polytechnic Institute (branch) Volgograd State Technical University,
Engels str., 42a, Volzhsky, Volgograd region, 404121, Russia

e-mail: mrsanytanittt@gmail.com, oxabra@yandex.ru

Abstract
This article raises the problem of the development of creative thinking of modern youth in the field of graphic design, and also examines the problems and solutions in the field of distance education. Research shows that the use of digital technologies in the educational process greatly changes the role of the teacher. On the other hand, modern students expect an increase in the interactivity of the educational process, the use of innovative digital solutions and the opportunity to show their creativity. The article discusses the concepts of gamification of education and creative thinking in relation to the field of graphic design training. Gamification in education is the use of gameplay as a learning method that allows students to improve their engagement and

increase their motivation to learn. On the other hand, the development of creative thinking - the ability to find unusual and effective solutions to problems – is also extremely important for future designers and artists. The article considers the ways of developing creative thinking in the process of teaching graphic design, identifies the problems of online education in general and graphic design training in particular. The final part of the article presents models of functional requirements for the implementation of a web system for teaching graphic design and the results of a study of potential users of such a system.
Keywords: online education; creative thinking; gamification of education; graphic design; training
For citation: Dmitrieva T.I., Abramova O.F. Research and analysis of the problems of developing creative thinking in the field of graphic design among modern youth // Research result. Information technologies. – T.8, №2, 2023. P. 18-25. DOI: 10.18413/2518-1092-2023-8-2-0-3

ВВЕДЕНИЕ

Современные технологии и информатизация изменили способы получения и восприятия информации. Особенно это относится к детям и подросткам, которые теперь получают информацию из различных электронных источников, таких как интернет. Кроме того, интернет – это место, где люди проводят свободное время, общаются и получают новые знания и навыки. В связи с этим, в учебный процесс начали внедряться новые системы, обеспечивающие доступность методических материалов в электронной форме. Это позволяет соответствовать современным реалиям и использовать новые способы обучения.

Как показывают исследования, использование цифровых технологий в учебном процессе сильно меняет роль педагога. Он перестает быть единственным носителем знаний и становится учебным менеджером и наставником, который направляет и поддерживает учеников в процессе обучения. Это позволяет ученикам учиться более эффективно и интересно.

ОСНОВНАЯ ЧАСТЬ

Цель работы: Снижение трудоемкости и повышение качества обучения графическому дизайну за счет автоматизации формирования адаптивной геймифицированной траектории обучения.

Материалы и методы исследования: Анализ литературных источников по теме развития креативного мышления и геймификации в образовании, исследование и анализ программных аналогов в области геймифицированного онлайн-обучения, функциональные методы исследования бизнес-процессов, объектно-ориентированные методы моделирования и проектирования программных систем.

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ И ИХ ОБСУЖДЕНИЕ

Сегодня молодое поколение больше всего привлекает интерактивность и возможность проявить свою креативность. Внедрение игровых элементов в процесс обучения помогает увеличить познавательную активность учеников, формировать интерес к знаниям и повышать мотивацию.

Геймификация в образовании – это использование игрового процесса как метода обучения, который позволяет улучшить вовлеченность учеников и повысить их мотивацию к обучению. Это происходит благодаря добавлению игровых элементов в учебный процесс, таких как система поощрений и рейтингов. Геймификация также помогает улучшить усидчивость и целеустремленность учеников, а также доводить задачи до финала и завершать их в назначенные сроки.

Зачем использовать геймификацию в процессе обучения? Чтобы сделать его более интересным и мотивирующим. Использование игровых механик позволяет объединить обучение и психологию, что повышает уровень внимательности, отдачи и сноровки у обучаемого. Кроме того,

наличие конкуренции в играх стимулирует обучаемого идти до конца и достигать лучших результатов [1].

Креативное мышление в графическом дизайне – это способность находить необычные и эффективные решения проблем дизайна [2].

Как и в других областях, творческое мышление в области графического дизайна можно улучшить через обучение и практику. Например, существуют определенные методы и подходы, которые могут способствовать развитию креативности. Рассмотрение проблем и различных способов использования объектов, создание множества концепций и идей без ограничения на традиционные методы, и работа в команде для обмена идеями, расширения кругозора и создания новых идей. Вот некоторые способы развития креативного мышления в графическом дизайне подробнее:

1) Использование дизайн-мышления. Дизайн-мышление – это методология решения проблем с помощью творческого процесса. Этот процесс включает пять фаз: понимание, наблюдение, определение проблемы, создание идеи и прототипа. Каждая фаза помогает дизайнерам развивать навыки творческого мышления и решать проблемы клиентов.

2) Изучение новых технологий и программ. Безусловно, изучение нового программного обеспечения для графического дизайна может помочь дизайнерам улучшить свои навыки и расширить кругозор. Например, изучение новых инструментов графического дизайна, таких как Adobe Photoshop, Illustrator, Sketch и Figma, поможет дизайнерам создавать более трендовые и востребованные решения.

3) Участие в конкурсах и соревнованиях по графическому дизайну поможет дизайнерам продемонстрировать свои текущие навыки и узнать много нового, а также получить опыт работы с различными проектами и клиентами [4].

4) Изучение работ других дизайнеров может помочь получить новые идеи и узнать востребованные фишки, а также найти вдохновение для своих собственных проектов. Ещё это поможет понять современные тенденции и стили [3].

5) Работа с различными материалами, такими как краски, карандаши и кисти, помогает дизайнерам не только не забывать навыки мелкой мотрики, но и находить новые идеи в чем-то обыденном и простом. Это также позволяет дизайнерам экспериментировать с различными стилями и техниками, чтобы оставаться креативными [3].

Из-за пандемии COVID-19, онлайн-образование стало обыденностью, и несмотря на множество преимуществ, таких как мобильность, удобство доступа, сокращение потребности в физической инфраструктуре, уменьшение затрат и повышение гибкости, с этим форматом связаны и определенные проблемы [5]. Вот некоторые из них:

1. Отсутствие реальной замены регулярному обучению.

Для множества студентов онлайн-образование является лишь формальностью, а не реальной альтернативой традиционному обучению. В некоторых случаях преподаватели просто предоставляют материалы учащимся, не занимаясь их обучением. Онлайн-тесты иногда основываются на принципе "разбирайся сам", что не способствует приобретению долгосрочных знаний у студентов [6].

2. Технические проблемы.

Многочисленные проблемы, связанные с онлайн-образованием, часто имеют техническую природу и касаются предоставления учебных программ студентам в разных регионах. Совместимость является одной из самых часто встречающихся проблем в онлайн-обучении. Она возникает, когда студенты из разных мест используют устройства с различными операционными системами. Даже устройства одного производителя могут функционировать на разных версиях одной и той же операционной системы [7].

3. Отсутствие самомотивации и навыков тайм-менеджмента.

Отсутствие самомотивации у студентов - причина незавершения онлайн-курсов. В онлайн-среде обучения меньше внешних факторов, которые могут подтолкнуть студентов к успеху. Учащиеся часто остаются наедине с собой во время учебы, и им не хватает внешней мотивации

для достижения целей обучения. Студенты на курсах дистанционного обучения часто изучают сложные материалы дома без дополнительного давления, связанного с традиционными колледжами. В результате соблюдение сроков в онлайн-обучении может быть сложным для студентов без сильной самомотивации и навыков управления временем [8].

4. Обилие отвлекающих факторов и отсутствие дисциплины.

Большинство студентов находят онлайн-обучение скучным и не мотивирующим. Учителя также могут столкнуться с нехваткой инструментов для создания увлекательных занятий, что приводит к потере интереса с обеих сторон. В онлайн-методе обучения отсутствует подотчетность, что может угрожать качеству образования. Отвлекающих факторов во время занятий много, часто за счет использования ноутбуков и мобильных телефонов [5].

Онлайн-образование имеет свои недостатки, но быстро развивается и совершенствуется. Для успеха в онлайн-среде обучения необходимо развивать сильную самомотивацию и дисциплинарные навыки. Онлайн-общение может заменить общение лицом к лицу с преподавателями, а взаимодействие между онлайн-студентами следует поощрять. Реализация практических студенческих проектов в сочетании с наставничеством является одним из наиболее эффективных способов развития практических навыков у онлайн-студентов [8]. Для точного определения наиболее проблематичных задач в организации, единственный способ - спросить. Это может быть выполнено через опросы, интервью, обзоры, анализ данных и т.д. Важно учитывать, что оценки онлайн-программ должны выходить за рамки измерения результатов обучения, чтобы исследовать, что конкретно мешает обучению [7].

В результате тщательного исследования инструментов и методов развития креативного мышления в процессе обучения графическому дизайну, а так же существующих программных аналогов был определен перечень функциональных и нефункциональных требований к системе. Разрабатываемая система будет иметь спрос, так как в ней предусмотрена реализация инструментов для развития креативности, демонстрации своих достижений с точки зрения потребителей разработанного курса, чего нет в системах аналогах, представленных в данный момент на рынке. Были определены бизнес-требования к проекту:

1) в системе должна быть возможность выкладывать тестовые задания для проверки полученных знаний;

2) в системе должна быть возможность не только писать в ней текстом, но и возможность прикладывать файлы типа docx, pdf, картинки формата jpeg, png, а также видеоматериалы в любом формате;

3) система должна формировать сертификат участника после прохождения учеником всего курса;

4) в системе должна быть возможность добавления графических работ учеников;

5) А так же определены бизнес-цели разработки:

6) увеличить число потребителей курса;

7) улучшить процесс восприятия информации и вовлеченность в процесс обучения участниками курса;

8) обеспечить удержание пользователей курса до конца обучения;

9) увеличить прибыль для создателей курса посредством того, что участники курса будут делиться своим опытом с другими людьми, будут советовать этот курс и тем самым привлекут новых пользователей.

Были выделены потенциальные пользователи системы: Преподаватель и Ученик. А так же составлены и проанализированы подробные карты пути в процессе обучения (Customer Journey Map, CJM) для каждой из выделенных групп. Пример CJM для пользователя Ученик приведен на рисунке 1.

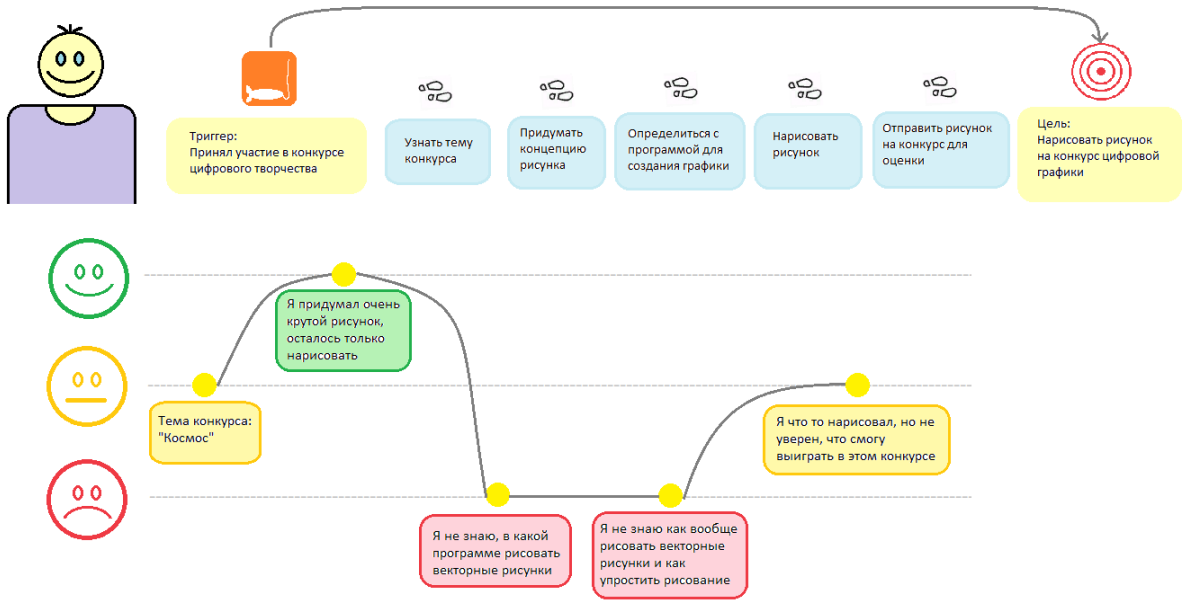

Рис. 1. Customer Journey Map потенциального пользователя Ученик по процессу «Обучение графическому дизайну»
Fig. 1. Customer Journey Map of a potential user Student in the process of "Teaching graphic design"

На основании проведенного анализа были разработаны модели функциональных требований в нотации UML и выделены экторы. Определена необходимость добавления эктора Администратор к уже вывленным Преподаватель и Ученик, диаграмма вариантов использования системы (use case) для которого представлена на рисунке 2.

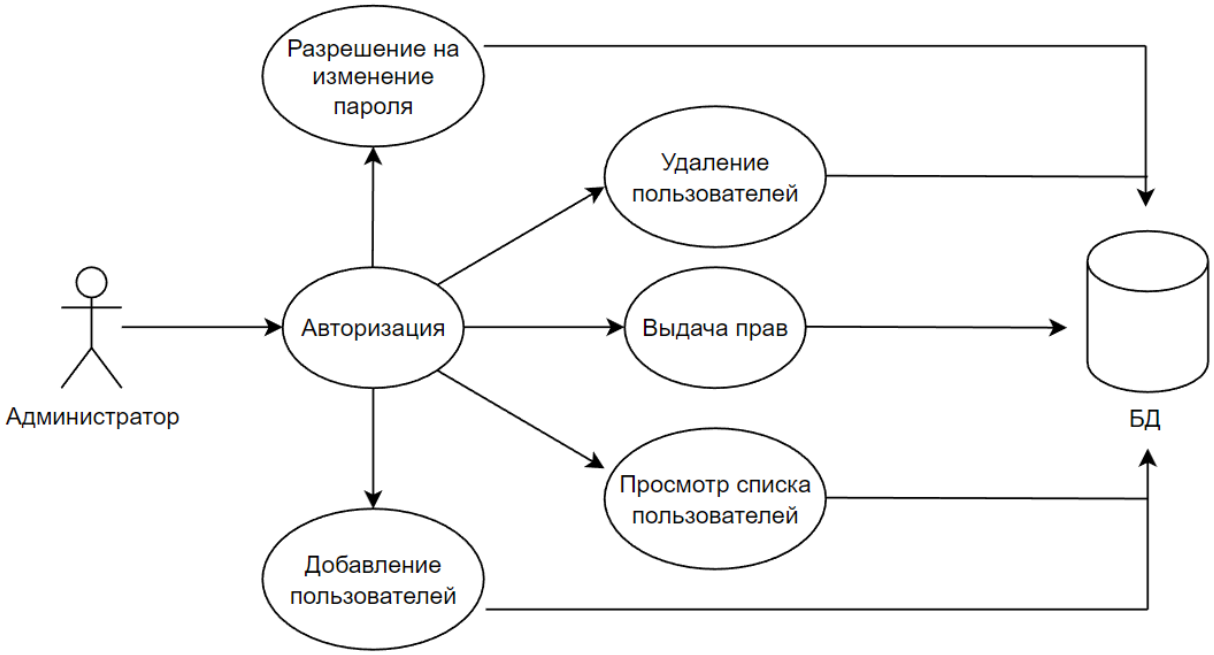

Рис. 2. Диаграмма функциональных требований к системе для эктора Администратор
Fig. 2. Diagram of functional system requirements for Ector Administrator

Модель вариантов использования системы для эктора Преподаватель представлена на рисунке 3.

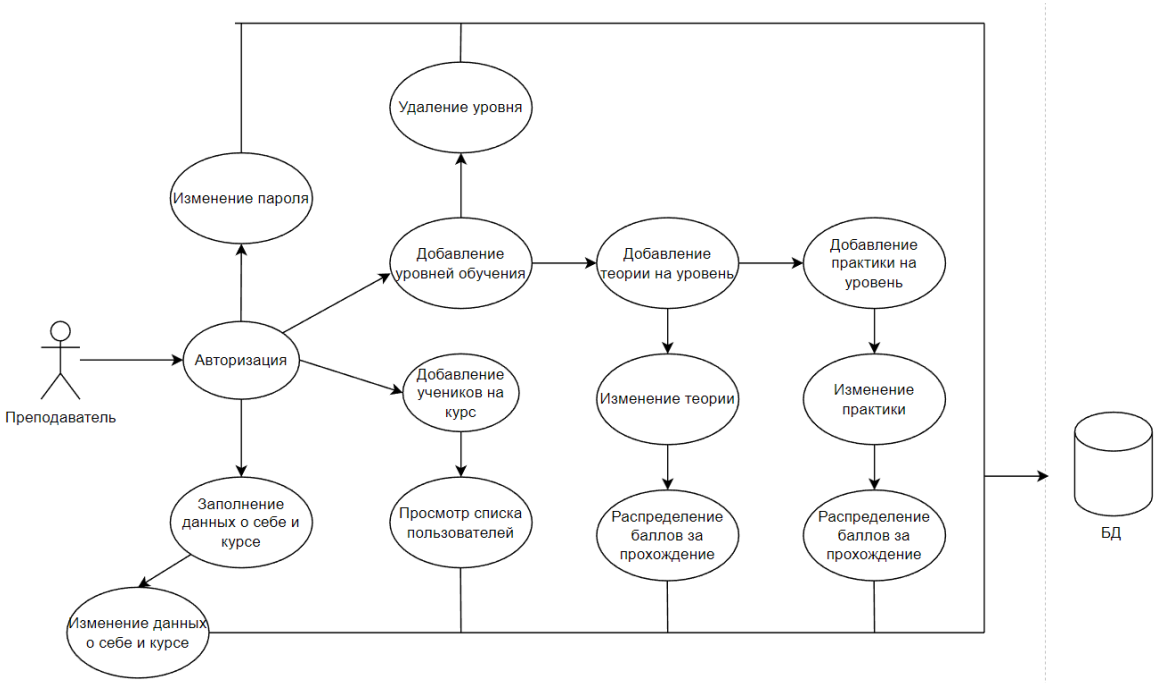

Рис. 3. Диаграмма функциональных требований к системе для эктора Преподаватель
Fig. 3. Diagram of functional system requirements for ector Teacher

Как видно из модели, у Преподавателя есть возможности управлять и отслеживать уровни обучения, регулируя наборы поощрительных баллов за прохождение отдельных этапов курса.

Модель вариантов использования для эктора Ученик представлена на рисунке 4.

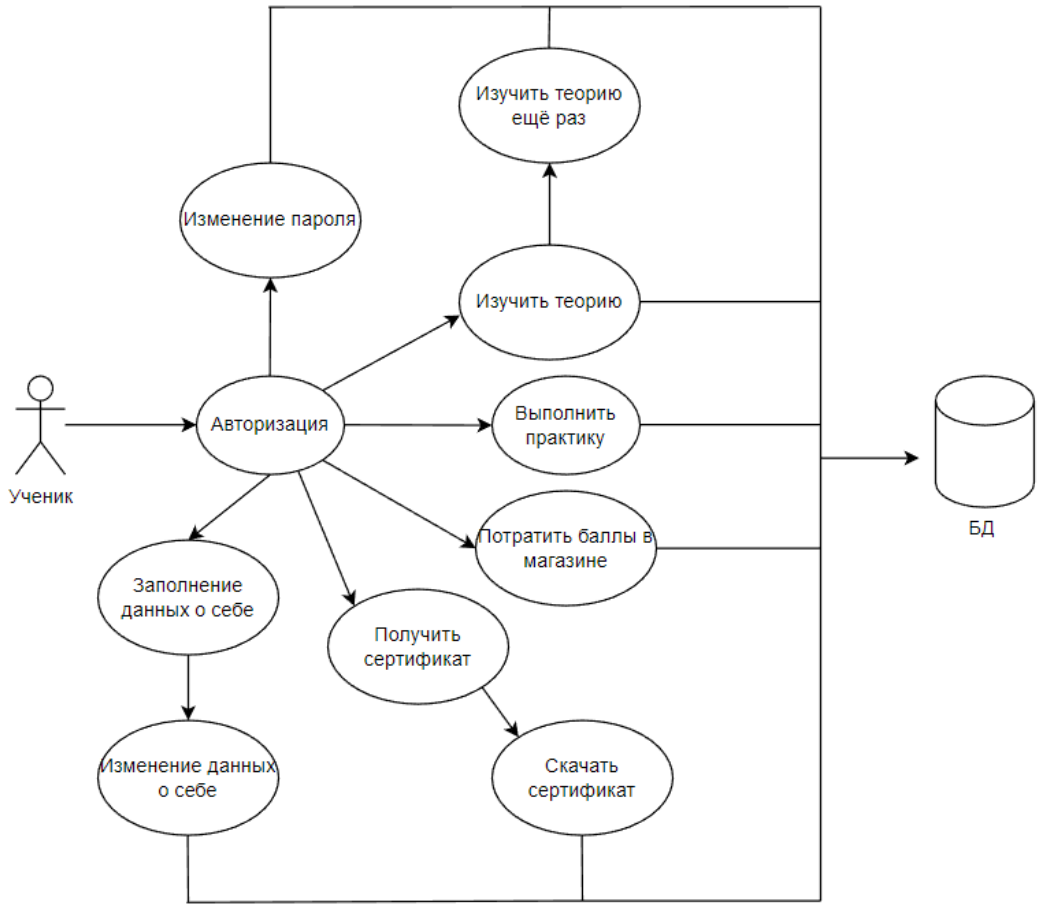

Рис. 4. Диаграмма функциональных требований к системе для эктора Ученик
Fig. 4. Diagram of the functional requirements for the system for the Student ector

Для повышения мотивации в веб-систему предлагается добавить возможность для Ученика использовать поощрительные баллы для приобретения дополнительного или развлекательного контента. Входные данные должны вводиться в систему посредством разработанных оконных форм, в которых должны быть представлены поля для ввода данных с возможностью валидации. Также должа быть реализована возможность добавления в систему таких файлов как: графический файл, видеофайл (ссылка на видео для экономии места в файловом хранилище сервера), текстовый файл формата txt, docx. Выходные данные представляют собой информацию о пользователях, информацию о курсах, загруженные в систему работы пользователей. Система должна формировать выходные данные в виде информации о пройденных курсах в профиле пользователя, полученные сертификаты, результаты прохождения тестирования, набранных поощрительных баллах и достигнутых уровнях.

ЗАКЛЮЧЕНИЕ

Внедрение онлайн-системы развития креативного мышления в области графического дизайна может решить несколько проблем в сфере образования:

1) онлайн-система может предоставить участникам инструменты для создания и обмена идеями в режиме реального времени;

2) система онлайн-образования позволяет учиться из любой точки мира, где есть доступ в Интернет. Это особенно актуально для тех, кто живет в отдаленных регионах, где нет возможности получить качественное образование;

3) даст возможность повысить креативный потенциал участников. Онлайн-система может предоставить доступ к учебным материалам, которые помогут применять техники креативного мышления на практике и использовать их для создания креативных решений;

4) увеличение доступности образования для людей с ограниченными возможностями, таких как люди с инвалидностью или маломобильные люди, которые могут испытывать трудности с перемещением в школу или университет;

5) улучшение качества образования. Система онлайн-образования может предоставлять учащимся доступ к выдающимся преподавателям мирового уровня;

6) экономия времени и денег: онлайн-образование позволяет учиться в любое время и месте, что экономит время и деньги на поездки в школу или университет.

Планируемая онлайн-система для обучения имеет большой круг применения и может быть использована не только для изучения графического дизайна, но и для других видов дисциплин. Основной круг пользователей, это те, кто интересуется рисованием, графикой и т.д. и кто не боится показывать остальным свое творчество.

Список литературы

1. Катков Д.С. Исследование и анализ применения принципов геймификации в обучающих программных системах [Электронный ресурс] / Д.С. Катков, О.Ф. Абрамова, А.А. Рыбанов // Постулат: электронный научный журнал. – 2019. – № 3. – 5 с. – Режим доступа: http://e-postulat.ru/index.php/Postulat/article/view/2518.

2. Мищук К., Креативное мышление: что это такое, как измерить и повысить свой потенциал [Электронный ресурс] // Хабр. – 2020. – URL: https://habr.com/ru/post/506620/ (дата обращения: 15.02.2023)

3. Ряженка М. Этапы дизайн мышления — подробный разбор 5 этапов по порядку [Электронный ресурс] // LeadStartup. – 2022. – URL: https://leadstartup.ru/db/design-thinking-phases (дата обращения: 16.02.2023)

4. 30 упражнений для развития креативного мышления [Электронный ресурс] // Quasa. – 2021. – URL: https://quasa.io/ru/media/30-uprazhneniy-dlya-razvitiya-kreativnogo-myshleniya (дата обращения: 15.02.2023)

5. Gutte N., What are the Biggest Challenges of Online Education Today? [Электронный ресурс] // Hurix. – 2023. – URL: https://www.hurix.com/what-are-the-biggest-challenges-facing-online-education-today/ (дата обращения: 16.03.2023)

6. Milosievski M., Zemon D., Stojkovska J., Popovski K., Learning Online: Problems and Solutions [Электронный ресурс] // Unicef. – 2020. – URL: https://www.unicef.org/northmacedonia/stories/learning-online-problems-and-solutions (дата обращения: 16.03.2023)

7. Willard J., 8 common challenges of online learning (and how to solve them) [Электронный ресурс] // Bigthink. – 2022. – URL: https://bigthink.com/plus/challenges-of-online-learning/ (дата обращения: 16.03.2023)

8. Tamm S., 10 Biggest Disadvantages of E-Learning [Электронный ресурс] // E-Student. – 2023. – URL: https://e-student.org/disadvantages-of-e-learning/ (дата обращения: 16.03.2023)

9. Абрамова О.Ф. Исследование методов развития инженерных способностей школьников / И.В. Ребро, Д.А. Мустафина, Г.А. Рахманкулова, О.Ф. Абрамова, Е.А. Перевалова, Т.А. Матвеева, Н.А. Соколова // Открытое и дистанционное образование. – 2019. – № 2 (74). – С. 5-11

10. Абрамова О.Ф. Анализ методов оценивания работ внеучебных конкурсных мероприятий, проводимых в дистанционном формате (Analysis of methods for evaluating the work of extra-curricular competitive events held in a remote format) / О.Ф. Абрамова, А.А. Рыбанов // Mathematics and Informatics = Математика и информатика (Болгария). – 2020. – Т. 63, № 6. – С. 665-671.

11. Цыганкова М.Л. К вопросу о повышении эффективности функционирования тренажёрно-обучающих систем / О.Ф. Абрамова, М.Л. Цыганкова // Открытое и дистанционное образование. – 2014. – № 4. – С. 34-39

12. Кувшинова Г.А. Особенности дизайн-образования в России / Г.А. Кувшинова // МНКО. –2021. – №4(89). – С. 130-133.

References

1. Katkov D.S. Research and analysis of the application of gamification principles in educational software systems [Electronic resource] / D.S. Katkov, O.F. Abramova, A.A. Rybanov // Postulate: electronic scientific journal. – 2019. – № 3. – 5 p. – URL: http://e-postulat.ru/index.php/Postulat/article/view/2518.

2. Mishchuk K., Creative thinking: what is it, how to measure and increase your potential [Electronic resource] // Habr. – 2020. – URL: https://habr.com/ru/post/506620/ (date access: 15.02.2023)

3. Ryazhenka M. Stages of design thinking - a detailed analysis of 5 stages in order [Electronic resource] // LeadStartup. – 2022. – URL: https://leadstartup.ru/db/design-thinking-phases (date access: 16.02.2023)

4. 30 creative thinking exercises [Electronic resource] // Quasa. – 2021. – URL: https://quasa.io/ru/media/30-uprazhneniy-dlya-razvitiya-kreativnogo-myshleniya (date access: 15.02.2023)

5. Gutte N., What are the Biggest Challenges of Online Education Today? [Electronic resource] // Hurix. – 2023. – URL: https://www.hurix.com/what-are-the-biggest-challenges-facing-online-education-today/ (date access: 16.03.2023)

6. Milosievski M., Zemon D., Stojkovska J., Popovski K., Learning Online: Problems and Solutions [Electronic resource] // Unicef. – 2020. – URL: https://www.unicef.org/northmacedonia/stories/learning-online-problems-and-solutions (date access: 16.03.2023)

7. Willard J., 8 common challenges of online learning (and how to solve them) [Electronic resource] // Bigthink. – 2022. – URL: https://bigthink.com/plus/challenges-of-online-learning/ (date access: 16.03.2023)

8. Tamm S., 10 Biggest Disadvantages of E-Learning [Electronic resource] // E-Student. – 2023. – URL: https://e-student.org/disadvantages-of-e-learning/ (date access: 16.03.2023)

9. Abramova O.F. Study of methods for the development of engineering abilities of schoolchildren / I.V. Rebro, D.A. Mustafina, G.A. Rakhmankulova, O.F. Abramova, E.A. Perevalova, T.A. Matveeva, N.A. Sokolova // Open and distance education. – 2019. – № 2 (74). – P. 5-11

10. Abramova O.F. Analysis of methods for evaluating the work of extra-curricular competitive events held in a remote format / O.F. Abramova, A.A. Rybanov // Mathematics and Informatics = Mathematics and Informatics (Bulgaria). – 2020. – T. 63, № 6. – P. 665-671.

11. Tsygankova M.L. On the issue of improving the efficiency of the functioning of training systems / O.F. Abramova, M.L. Tsygankova // Open and distance education. – 2014. – № 4. – P. 34-39

12. Kuvshinova G.A. Features of design education in Russia / G.A. Kuvshinova // MNKO. – 2021. – No.4(89). – P. 130-133.

Дмитриева Татьяна Игоревна, студент кафедры «Информатика и технология программирования»
Абрамова Оксана Федоровна, доцент кафедры «Информатика и технология программирования»

Dmitrieva Tatiana Igorevna, student of the Department of Informatics and Programming Technology
Abramova Oksana Fedorovna, Associate Professor of the Department of Informatics and Programming Technology

АВТОМАТИЗАЦИЯ И УПРАВЛЕНИЕ
AUTOMATION AND CONTROL

УДК 004 **DOI: 10.18413/2518-1092-2022-8-2-0-4**

Руслякова К.А.
Свиридова О.В.

О МОДЕЛИРОВАНИИ ДЕЯТЕЛЬНОСТИ АДМИНИСТРАТОРА САЛОНА КРАСОТЫ

Волжский политехнический институт (филиал) ФГБОУ ВО «Волгоградский государственный технический университет», ул. Энгельса, д. 42а, г. Волжский, Волгоградская область, 404121, Россия

e-mail: ksenya.ruslyakova@yandex.ru, osviridova@inbox.ru

Аннотация
В статье было проведено исследование и анализ проблем, возникающих в процессе деятельности администратора салона красоты. Администратор играет важную роль в эффективной работе организации и улучшении качества обслуживания клиентов. Он занимается составлением графика работы, контролирует стоимость услуг и качество работы мастеров, отвечает за наличие расходных материалов на складе, обеспечивает высокий уровень обслуживания клиентов начиная от консультации и бронированием записи на процедуру, заканчивая принятием оплаты реализованной услуги. Как показывают исследования, рынок салонов красоты активно развивается в настоящее время и поток клиентов увеличивается, вместе с этим увеличивается и загруженность администратора. Важно помогать администратору выполнять свои рабочие обязанности эффективно, чтобы получать максимальную прибыль и улучшать имидж салона. В статье были выделены обязанности администратора, приведены и смоделированы основные бизнес-процессы салона красоты при предоставлении услуг, описаны причины актуальности разработки автоматизированной системы и проблемы, которые будут решены после ее внедрения.
Ключевые слова: салон красоты; индустрия красоты; автоматизированное рабочее место; обязанности администратора; информационная система
Для цитирования: Руслякова К.А., Свиридова О.В. О моделировании деятельности администратора салона красоты // Научный результат. Информационные технологии. – Т.8, №2, 2023. С. 26-34. DOI: 10.18413/2518-1092-2022-8-2-0-4

Ruslyakova K.A.
Sviridova O.V.

ABOUT MODELING THE ACTIVITY OF A BEAUTY SALON ADMINISTRATOR

Volzhsky Polytechnic Institute (branch) Volgograd State Technical University,
Engels str., 42a, Volzhsky, Volgograd region, 404121, Russia

e-mail: ksenya.ruslyakova@yandex.ru, osviridova@inbox.ru

Abstract
The article conducted a study and analysis of the problems that arise in the course of the activities of the beauty salon administrator. The administrator plays an important role in the effective work of the organization and improving the quality of customer service. He is engaged in drawing up a work schedule, controls the cost of services and the quality of work of craftsmen, is responsible for the availability of consumables in stock, provides a high level of customer service from consulting and booking an appointment for the procedure, ending with accepting payment for the service implemented. According to research, the beauty salon market is actively developing at the moment and the flow of customers is increasing, along with this, the workload of the administrator is also increasing. It is important to help the administrator to perform his work duties effectively in order to maximize profits and improve the image of the salon. The article highlighted the responsibilities of the administrator, presented and modeled the main business

processes of the beauty salon in the provision of services, described the reasons for the relevance of the development of an automated system and the problems that will be solved after its implementation.
Keywords: beauty salon; beauty industry; automated workplace; administrator responsibilities; information system
For citation: Ruslyakova K.A., Sviridova O.V. About modeling the activity of a beauty salon administrator // Research result. Information technologies. – T.8, №2, 2023. – P. 26-34. DOI: 10.18413/2518-1092-2022-8-2-0-4

ВВЕДЕНИЕ

Салон красоты – это место, где можно получить профессиональную помощь в уходе за своей внешностью. В салоне красоты можно провести процедуры, которые трудно сделать дома, например, окрашивание и укладка волос, маникюр и педикюр, массаж, наращивание ресниц, профессиональный макияж и многое другое [13]. В салоне работают профессиональные мастера и стилисты, которые помогут подобрать индивидуальную программу ухода и сделают все, чтобы клиенты чувствовали себя красивыми и ухоженными. За организацию и контроль работы салона красоты отвечает администратор. Он занимается многими аспектами управления бизнесом: от общения с клиентами до управления мастерами.

Многие люди посещают салоны красоты регулярно, чтобы поддерживать свой внешний вид и здоровье, которые в последнее время особенно актуальны и являются синонимом успешности.

Согласно исследованию, проведенному компанией NeoAnalytics, к 2021 году рынок парикмахерских и салонов красоты полностью восстановился после кризиса: объем рынка вырос на 46,9% и составил более 150 млрд рублей. Согласно данным исследования, только 45% населения регулярно посещают салоны, следовательно, рынок салонов красоты в России не насыщен и имеет возможности для развития [12].

Увеличение потока клиентов в салонах красоты может привести к большой загруженности администратора, особенно в тех случаях, когда управление записями клиентов и расписанием мастеров происходит вручную. На данный момент во многих организациях этой сферы отсутствует автоматизация бизнес-процессов, причиной этого может быть нехватка достойных программных решений с необходимым функционалом для решения всевозможных проблем.

Отсутствие автоматизации бизнес-процессов может стать серьезным препятствием для эффективного функционирования бизнеса и привести к трудностям в процессе клиентского обслуживания и контроле качества работы, что может отразиться на репутации салона и потере потенциальных клиентов [6]. В связи с этим, стоит рассмотреть вопрос о внедрении современных автоматизированных систем для администратора салона красоты, которые помогут улучшить качество обслуживания, повысить эффективность работы мастеров и снизить погрешности и ошибки в управлении бизнесом.

ОСНОВНАЯ ЧАСТЬ

Для выявления и анализа проблем в деятельности администратора салона красоты необходимо произвести исследование предметной области. Рассмотрим организационную структуру салона красоты (рис. 1):

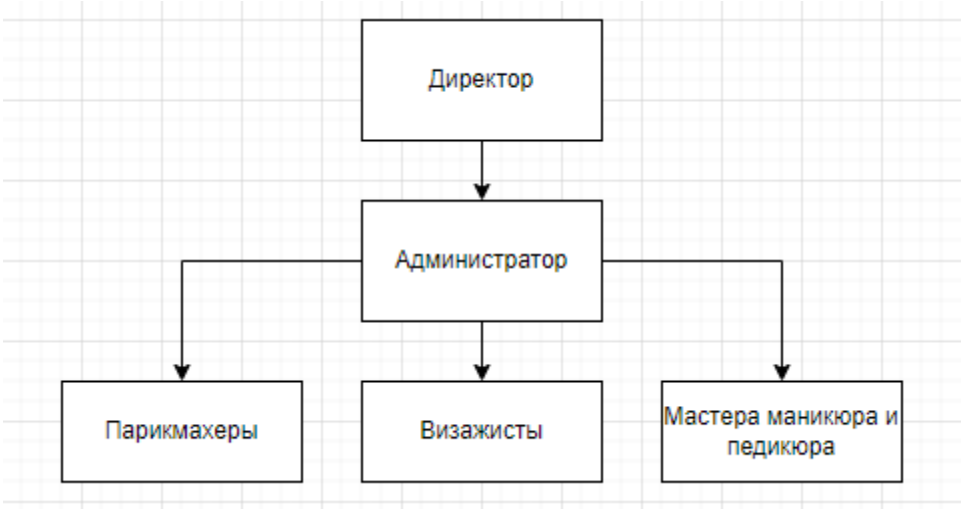

Рис. 5. Организационная структура салона красоты
Fig. 1. Organizational structure of the beauty salon

Как видно на рисунке, администратор салона красоты находится в подчинении директора, а мастера – в подчинении администратора. Таким образом, администратор является ключевым звеном в управлении работой мастеров и организации работы салона в целом.

На рис. 2 представлена общая функциональная модель IDEF0 процесса «Предоставление косметических услуг», которая отражает общий принцип работы салона красоты.

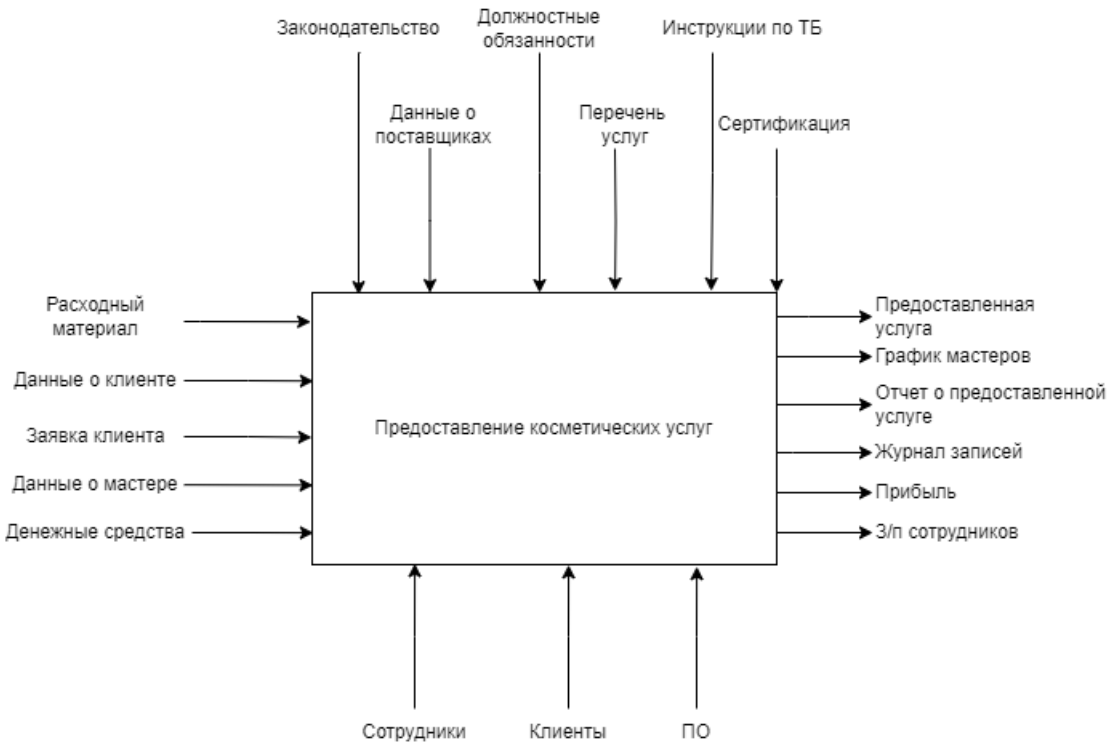

Рис. 2. Общая функциональная модель IDEF0 процесса «Предоставление косметических услуг»
Fig. 2. General functional model IDEF0 of the process "Provision of cosmetic services"

Для предоставления услуг требуется заявка от клиента на предоставление определенной процедуры и его данные, данные о мастере, а также информация о необходимых материалах для реализации этой процедуры. Ресурсами данного процесса являются сотрудники – администратор и мастера, клиенты и программное обеспечение, которое включает в себя оборудование, инструменты и приспособления, используемые при предоставлении услуги. Управленческими

потоками данных выступают законодательство, должностные обязанности сотрудников, нормативные документы, данные о поставщиках, перечень услуг и график работы мастеров. В результате после реализации услуги будет выписан чек клиенту, получена прибыль, в журнале посещений будет новая отметка о предоставленной услуге и израсходованном материале, выплачена зарплата сотрудникам.

Для более углубленного анализа рассмотрим декомпозицию общей функциональной модели IDEF0 на рис. 3.

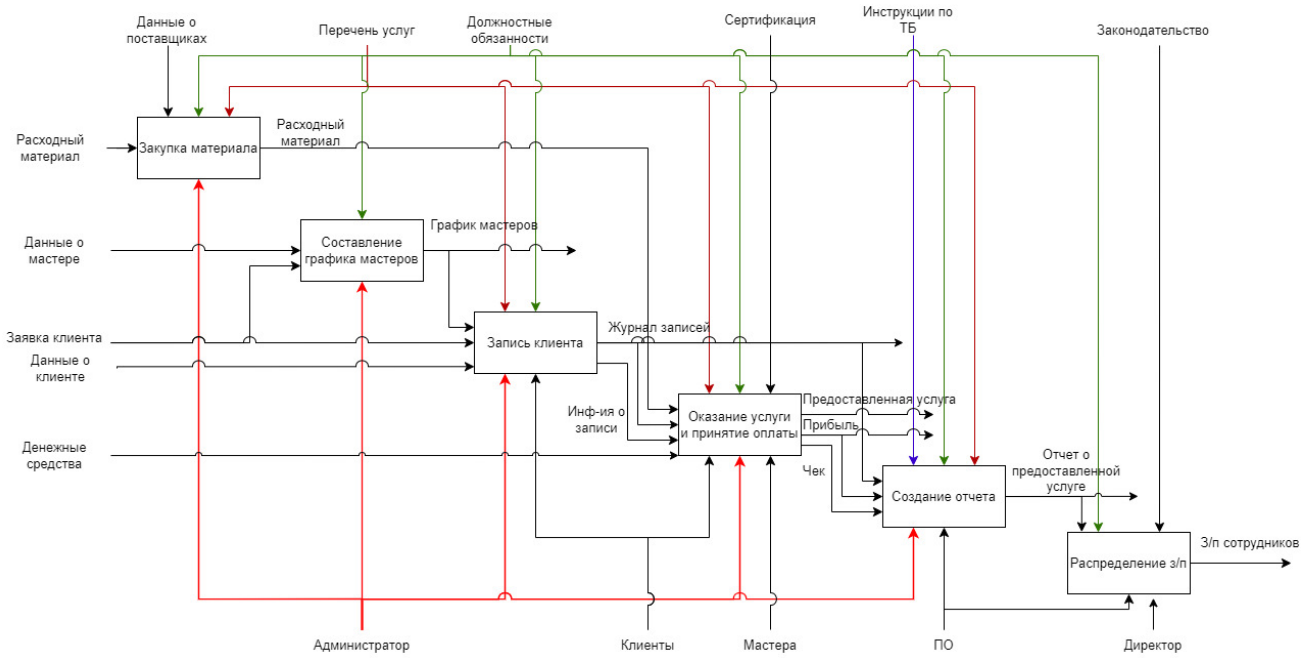

Рис. 3. Декомпозиция общей функциональной модели IDEF0 процесса «Предоставление косметических услуг»

Fig. 3. Decomposition of the general functional model IDEF0 of the process "Provision of cosmetic services"

Модель отражает внутреннюю структуру процесса «Предоставление косметических услуг», исходя из которой можно увидеть, что он состоит из следующих подпроцессов: закупка материала; составление графика мастеров; запись клиента; оказание услуги и принятие оплаты; создание отчета; распределение заработной платы.

В обязанности администратора входят:

1. Прием звонков, консультация клиентов и запись на прием;
2. Составление графика работы мастеров, распределение клиентов между мастерами и контроль качества выполнения услуг;
3. Оформление документов и контроль финансовых операций;
4. Работа с клиентской базой данных и рассылка актуальных акций и предложений;
5. Ведение учета оборудования, инвентаря и материалов на складе.

Одна из важных задач администратора салона красоты - обеспечить высокий уровень обслуживания клиентов, чтобы привлекать новых клиентов и удерживать текущих [20].

В ходе исследования предметной области было проведено интервьюирование с администратором салона красоты, в ходе которого были выявлены потребности и проблемы, с которыми он сталкивается при выполнении определенных задач, и отражены в карте пути пользователя (Customer Journey Map, CJM) на рис. 4.

Рис. 4. Customer Journey Map администратора салона красоты в процессе выполнениях своих обязанностей

Fig. 4. Customer Journey Map of the beauty salon administrator in the process of performing their duties

В своей работе администратор может столкнуться с множеством проблем в связи с загруженностью из-за большого объема должностных обязанностей или при высоком потоке клиентов [2]. Рассмотрим наиболее значимые проблемы при развитии салона красоты:

1. Недостаточное время на консультацию и учет всех пожеланий клиента из-за большой посещаемости салона и большому количеству обязанностей у администратора. Недовольство качеством обслуживания может привести к потере потенциальных клиентов.
2. Информация о клиенте и его записи могут быть утеряны.
3. Ошибки в распределении нагрузки на персонал при составлении графика, что может привести к перегрузке отдельных сотрудников и затруднениям в управлении рабочим процессом. Также администратор может случайно назначить двух клиентов на один и тот же период времени или ошибиться в предоставлении информации клиенту.
4. Неправильный учет и несвоевременное пополнение количества материалов на складе, что может привести к нехватке запасов, задержкам и отказам в обслуживании, недовольству клиентов.
5. Несвоевременное принятие мер по предотвращению порчи материалов. При порче материалов салон может испытывать финансовые потери.

Важно помогать администратору выполнять свои рабочие обязанности эффективно, чтобы получать максимальную прибыль и улучшать имидж салона. В настоящее время одним из решений проблем, связанных с организацией работы в салоне красоты и улучшения качества обслуживания клиентов, может стать автоматизированное рабочее место администратора [7].

Данная система предоставляет полезные функции, такие как:

- онлайн-запись на сайте, что позволяет клиентам быстро записываться на услуги онлайн без необходимости стоять в длинных очередях на стойках регистрации или звонить администратору и общаться лично по телефону;
- контроль за графиком работы мастеров, что позволяет администратору отслеживать отработанное время;
- обработка информации о проведенных услугах,
- проведение учета материалов, позволяющее всегда точно поддерживать уровень запасов на складе, и прочих расходов салона;
- статистика общих показателей эффективности, таких как общий доход, полученный за месяц / год, средняя стоимость заказа, количество постоянных клиентов и другое, что помогает

администратору принимать обоснованные решения о том, как наилучшим образом распределять ресурсы внутри салона;

- получение информации о клиентах, например, история посещений, услуги, приобретенные в прошлом, контактные данные для последующих звонков или электронных писем. Эта информация поможет легко создавать персонализированные рекламные акции, адаптированные к потребностям каждого отдельного клиента, что приведет к более высокому уровню конверсии продаж у существующих клиентов, а также к повышению уровня лояльности среди них.

ЗАКЛЮЧЕНИЕ

С использованием автоматизированного рабочего места администратором его рабочие задачи становятся намного проще в выполнении. Система позволяет снизить временные затраты на выполнение бизнес-процессов за счет устранения ручного труда, связанного с самостоятельным поиском свободного времени на услугу при консультации клиента. Кроме того, это позволило бы администраторам сосредоточиться на предоставлении более качественных услуг, а не тратить время на рутинные обязанности, которые снижают их производительность в других областях, требующих внимания.

Система помогла бы обеспечить точность при работе с личной информацией клиентов, поскольку все данные надежно хранятся онлайн вместо бумажных записей, которые со временем могут быть потеряны или повреждены из-за износа или стихийных бедствий.

Наконец, наличие автоматизированной системы помогает обеспечить согласованность во всех операциях, чтобы все сотрудники знали, какие задачи перед ними стоят в ближайшее время – это устраняет ошибки, вызванные человеческим фактором, одновременно повышая общую эффективность в коллективе в целом.

Автоматизированные системы сегодня становятся все более популярными, поскольку они обеспечивают преимущества экономии средств наряду с улучшением качества обслуживания клиентов - то, что администраторам следует рассмотреть для внедрения, если они хотят, чтобы их салоны красоты работали бесперебойно.

Список литературы

1. 7 бизнес-процессов салона красоты, которые надо автоматизировать в первую очередь [Электронный ресурс] // SendPulse. – 2019. – URL: https://sendpulse.com/ru/blog/beauty-salon-automation(дата обращения: 15.03.2023).

2. 9 ошибок администратора салона красоты, которые убивают продажи [Электронный ресурс] // Beauty Pro. – URL: https://beautyprosoftware.com/ru/blog/russkij-9-oshibok-administratora-salona-krasoty-kotorye-ubivajut-prodazhi/ (дата обращения: 03.03.2023).

3. CRM для салона красоты: функции, возможности и интересные «фишки» [Электронный ресурс] // Manzana Group. – 2022. – URL: https://manzanagroup.ru/information/crm-dlya-salona-krasoty-funktsii-vozmozhnosti-i-interesnye-fishki/(дата обращения: 11.03.2023).

4. Абсатаров Р.Н., Абрамова О.Ф. Исследование деятельности сервисного центра компьютерной техники и анализ осуществимости автомаизации бизнес-процессов // Научное обозрение. Технические науки. – 2020. – № 5. – С. 5-10; URL: https://science-engineering.ru/ru/article/view?id=1309 (дата обращения: 30.03.2023).

5. Автоматизация бизнес-процессов [Электронный ресурс] // Unisender. – 2021. – URL: https://www.unisender.com/ru/glossary/chto-takoe-avtomatizacija-business/(дата обращения: 08.02.2023).

6. Автоматизация процессов: кому нужна, кто её проводит и какие системы для неё использовать [Электронный ресурс] // Skillbox Media. – 2022. – URL: https://skillbox.ru/media/management/avtomatizatsiya-protsessov-komu-nuzhna-kto-eye-provodit-i-kakie-sistemy-dlya-neye-ispolzovat/(дата обращения: 11.03.2023).

7. Автоматизация управления персоналом: виды, выбор программы и аналоги [Электронный ресурс] // Envybox Блог. – 2020. – URL: https://envybox.io/blog/avtomatizacija-upravlenija-personalom/ (дата обращения: 30.03.2023).

8. Анализ рынка парикмахерских и салонов красоты в России в 2017-2021 гг., прогноз на 2022-2026 гг. Детализация по городам. Перспективы рынка в условиях санкций [Электронный ресурс] // BusinesStat. – 2022. – URL: https://businesstat.ru/images/demo/beauty_salons_russia_demo_businesstat.pdf(дата обращения: 15.01.2023).

9. Бородина И.О., Макушкина Л.А., Рыбанов А.А. Разработка автоматической системы учета рабочего времени сотрудников организации на основании фонового анализа их действий // Материалы X Международной студенческой научной конференции «Студенческий научный форум». – 2018. – URL: https://scienceforum.ru/2018/article/2018001712 (дата обращения: 17.03.2023).

10.В России выросло число салонов красоты [Электронный ресурс] // RG. – 2023. – URL: https://rg.ru/2023/03/20/dela-idut-krasivo.html(дата обращения: 10.02.2023).

11.График работы: шаги для эффективного планирования сотрудников [Электронный ресурс] // Business Yield. – 2022. – URL: https://businessyield.com/ru/management/work-schedule/(дата обращения: 10.02.2023).

12.Динамику развития салонов красоты [Электронный ресурс] // New Style Sound. – 2022. – URL: https://nssound.ru/zvuk/dinamiku-razvitiya-salonov-krasoty/(дата обращения: 15.01.2023).

13.Индустрия красоты [Электронный ресурс] // ВсеТренинги.ру. – URL: https://vsetreningi.ru/schools/industriya_krasoty/ (дата обращения: 28.01.2023).

14.Кадырова Д.Д., Васева Е.С. Определение Функциональных требований к системе учета работы студии красоты «BEAUTY ROOM» // Научное обозрение. Технические науки. – 2022. – № 4. – С. 28-33; URL: https://science-engineering.ru/ru/article/view?id=1406 (дата обращения: 01.04.2023).

15.Мазуренко Н.А., Свиридова О.В., Рыбанов А.А. Обзор программных средств автоматизации документооборота // Материалы XI Международной студенческой научной конференции «Студенческий научный форум». – 2019. – URL: https://scienceforum.ru/2019/article/2018012703 (дата обращения: 01.03.2023).

16.Овчаров, Д.С. Исследование и разработка алгоритмов автоматизированной системы для онлайн-записи на прием к нотариусу и подготовки шаблонов документов / Д.С. Овчаров, О.В. Свиридова. — Текст: электронный // NovaInfo, 2017. — № 58. — С. 72-78. — URL: https://novainfo.ru/article/10827 (дата обращения: 26.02.2023).

17.Пронин И.В. Автоматизированные системы управления предприятием (АСУП) // Материалы XII Международной студенческой научной конференции «Студенческий научный форум». – 2020. – URL: https://scienceforum.ru/2020/article/2018018742 (дата обращения: 17.03.2023).

18.Российский рынок парикмахерских и салонов красоты: итоги 2021 г., прогноз до 2025 г. [Электронный ресурс] // BusinesStat. – 2022. – URL: https://www.neoanalytics.ru/wp-content/uploads/2022/02/demo_neoanalytics_rossijskij-rynok-parikmaherskih-i-salonov-krasoty_2022.pdf(дата обращения: 15.01.2023).

19.Средства и преимущества автоматизации красивого бизнеса: почему салоны отказываются от Excel [Электронный ресурс] // Директор салона красоты. – 2018. – URL: https://www.dirsalona.ru/article/1201-sredstva-i-preimushchestva-avtomatizatsii-krasivogo-biznesa-pochemu-salony-otkazyvayutsya-ot(дата обращения: 08.02.2023).

20.Что входит в обязанности администратора салона красоты? [Электронный ресурс] // Salon Secret. – URL: https://www.salonsecret.ru/for-hairdressers/obyazannosti-administratora-salona-krasoty (дата обращения: 10.02.2023).

21.Что нужно знать и уметь администратору салона красоты [Электронный ресурс] // Nails Журнал. – 2022. – URL: https://nails-mag.ru/biznes/administrator-salona-krasoty/(дата обращения: 15.03.2023).

References

1. 7 beauty salon business processes that need to be automated first [Electronic resource] // SendPulse. - 2019. – URL: https://sendpulse.com/ru/blog/beauty-salon-automation (date of application: 03/15/2023).

2. 9 errors of the beauty salon administrator that kill sales [Electronic resource] // Beauty Pro. – URL: https://beautyprosoftware.com/ru/blog/russkij-9-oshibok-administratora-salona-krasoty-kotorye-ubivajut-prodazhi / (date of application: 03.03.2023).

3. CRM for a beauty salon: functions, features and interesting "chips" [Electronic resource] // Manzana Group. – 2022. – URL: https://manzanagroup.ru/information/crm-dlya-salona-krasoty-funktsii-vozmozhnosti-i-

interesnye-fishki/(date of application: 11.03.2023).

4. Absatarov R.N., Abramova O.F. Research of the activity of the computer equipment service center and analysis of the feasibility of automatization of business processes // Nauchnoe obozrenie. Tekhnicheskie nauki. – 2020. – No. 5. – PP. 5-10; URL: https://science-engineering.ru/ru/article/view?id=1309 (date of application: 30.03.2023).

5. Automation of business processes [Electronic resource] // Unisender. – 2021. – URL: https://www.unisender.com/ru/glossary/chto-takoe-avtomatizacija-business / (date of application: 08.02.2023).

6. Process automation: who needs it, who conducts it and what systems to use for it [Electronic resource] // Skillbox Media. – 2022. – URL: https://skillbox.ru/media/management/avtomatizatsiya-protsessov-komu-nuzhna-kto-eye-provodit-i-kakie-sistemy-dlya-neye-ispolzovat/ (date of application: 11.03.2023).

7. Automation of personnel management: types, program selection and analogues [Electronic resource] // Envybox Blog. – 2020. – URL: https://envybox.io/blog/avtomatizacija-upravlenija-personalom / (date of application: 30.03.2023).

8. Analysis of the market of hairdressers and beauty salons in Russia in 2017-2021, forecast for 2022-2026. Details by city. Market prospects under sanctions [Electronic resource] // Businessstat. – 2022. – URL: https://businesstat.ru/images/demo/beauty_salons_russia_demo_businesstat.pdf (date of application: 15.01.2023).

9. Borodina I.O., Makushkina L.A., Rybanov A.A. Development of an automatic system for recording the working hours of employees of the organization based on background analysis of their actions // Materialy X Mezhdunarodnoj studencheskoj nauchnoj konferencii «Studencheskij nauchnyj forum». – 2018. – URL: https://scienceforum.ru/2018/article/2018001712 (date of application: 03/17/2023).

10. The number of beauty salons has grown in Russia [Electronic resource] // RG. – 2023. – URL: https://rg.ru/2023/03/20/dela-idut-krasivo.html (date of application: 10.02.2023).

11. Work schedule: steps for effective employee planning [Electronic resource] // Business Yield. – 2022. – URL: https://businessyield.com/ru/management/work-schedule / (date of application: 10.02.2023).

12. Dynamics of the development of beauty salons [Electronic resource] // New Style Sound. – 2022. – URL: https://nssound.ru/zvuk/dinamiku-razvitiya-salonov-krasoty / (date of application: 15.01.2023).

13. Beauty industry [Electronic resource] // VseTreningi.ru. – URL: https://vsetreningi.ru/schools/industriya_krasoty / (date of application: 28.01.2023).

14. Kadyrova D.D., Vaseva E.S. Definition of functional requirements for the accounting system of the beauty studio "BEAUTY ROOM" // Nauchnoe obozrenie. Tekhnicheskie nauki. – 2022. – No. 4. – PP. 28-33; URL: https://science-engineering.ru/ru/article/view?id=1406 (date of application: 01.04.2023).

15. Mazurenko N.A., Sviridova O.V., Rybanov A.A. Overview of software tools for document management automation // Materialy X Mezhdunarodnoj studencheskoj nauchnoj konferencii «Studencheskij nauchnyj forum». – 2019. – URL: https://scienceforum.ru/2019/article/2018012703 (date of application: 01.03.2023).

16. Ovcharov, D.S. Research and development of algorithms of an automated system for online appointment with a notary and preparation of document templates / D.S. Ovcharov, O.V. Sviridova. — Text: electronic // NovaInfo, 2017. — No. 58. — pp. 72-78. — URL: https://novainfo.ru/article/10827 (date of application: 02/26/2023).

17. Pronin I.V. Automated enterprise management systems (ASUP) // Materialy X Mezhdunarodnoj studencheskoj nauchnoj konferencii «Studencheskij nauchnyj forum». – 2020. – URL: https://scienceforum.ru/2020/article/2018018742 (date of application: 03/17/2023).

18. The Russian market of hairdressers and beauty salons: results of 2021, forecast to 2025 [Electronic resource] // Businessstat. – 2022. – URL: https://www.neoanalytics.ru/wp-content/uploads/2022/02/demo_neoanalytics_rossijskij-rynok-parikmaherskih-i-salonov-krasoty_2022.pdf(date of application: 15.01.2023).

19. Means and advantages of automation of a beautiful business: why salons refuse Excel [Electronic resource] // Direktor salona krasoty. – 2018. – URL: https://www.dirsalona.ru/article/1201-sredstva-i-preimushchestva-avtomatizatsii-krasivogo-biznesa-pochemu-salony-otkazyvayutsya-ot(date of application: 08.02.2023).

20. What is the responsibility of the beauty salon administrator? [Electronic resource] // Salon Secret. – URL: https://www.salonsecret.ru/for-hairdressers/obyazannosti-administratora-salona-krasoty (date of application: 10.02.2023).

21. What a beauty salon administrator needs to know and be able to do [Electronic resource] // Nails Magazine. – 2022. – URL: https://nails-mag.ru/biznes/administrator-salona-krasoty / (date of application: 03/15/2023).

Руслякова Ксения Алексеевна, студент кафедры «Информатика и технология программирования»
Свиридова Ольга Викторовна, кандидат технических наук, доцент кафедры «Информатика и технология программирования»

Ruslyakova Ksenia Alekseevna, student of the Department of Informatics and Programming Technology
Sviridova Olga Viktorovna, Candidate of Technical Sciences, Associate Professor of the Department of Informatics and Programming Technology

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И ПРИНЯТИЕ РЕШЕНИЙ
ARTIFICIAL INTELLIGENCE AND DECISION MAKING

УДК 004.8 **DOI: 10.18413/2518-1092-2022-8-2-0-5**

Крайновских В.И.[1]
Комарова А.А.[2]
Басов О.О.[2]

МЕТОД ВЫЯВЛЕНИЯ КОСВЕННЫХ ПРИЗНАКОВ КОРРУПЦИОННЫХ ДЕЯНИЙ ПО ВИДЕОЗАПИСЯМ ВЫСТУПЛЕНИЙ ГОССЛУЖАЩИХ

[1)] Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет «Высшая школа экономики», ул. Кантемировская дом 3, корп.1, лит. А, г. Санкт–Петербург, 194100, Россия
[2)] Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики», Кронверкский пр., д. 49, г. Санкт-Петербург, 197101, Россия

e-mail: vikraynova@edu.hse.ru

Аннотация
На данный момент проблема противодействию коррупционным действиям в сфере государственной службы по–прежнему не теряет свою актуальность. Предполагается, что при совершении коррупционных деяний люди проявляют определенные вербальные и невербальные сигналы, с помощью которых можно выявить коррупционные признаки. В статье рассматривается проблема нарушения антикоррупционного законодательства в государственных и муниципальных учреждениях с точки зрения психоэмоционального состояния чиновников. Предлагается использовать методы машинного обучения для анализа видео и аудио записей выступлений с неподготовленной речью чиновников различного уровня власти, где они отвечают на вопросы журналистов и общественности, с целью определения эмоций и выявления агрессии, неуверенности, а также уклончивости в ответах. Результаты исследования могут быть полезны для государственных органов, занимающихся борьбой с коррупцией, а также для общественности, заинтересованной в прозрачности и честности деятельности государственных служащих.
Ключевые слова: противодействие коррупции; государственное управление; машинное обучение; вербальный анализ; анализ аудио-видеозаписей; анализ психоэмоционального состояния
Для цитирования: Крайновских В.И., Комарова А.А., Басов О.О. Метод выявления косвенных признаков коррупционных деяний по видеозаписям выступлений госслужащих // Научный результат. Информационные технологии. – Т.8, №2, 2023. – С. 35-45. DOI: 10.18413/2518-1092-2022-8-2-0-5

Krainovskikh V.I.[1]
Komarova A.A.[2]
Basov O.O.[2]

THE METHOD OF IDENTIFYING INDIRECT SIGNS OF CORRUPTION ACTS BASED ON VIDEO RECORDINGS OF SPEECHES OF CIVIL SERVANTS

[1)] Federal State Autonomous Educational Institution of Higher Education "National Research University "Higher School of Economics", 3 Kantemirovskaya str., building 1, lit. A, St. Petersburg, 194100, Russia
[2)] Saint Petersburg National Research University of Information Technologies, Mechanics and Optics, 49 Kronverkskiy prospekt, St. Petersburg, 197101, Russia

e-mail: vikraynova@edu.hse.ru

Abstract
At the moment, the problem of countering corruption in the field of public service still does not lose its relevance. It is assumed that when committing acts of corruption, people show certain verbal and non-verbal signals, with the help of which it is possible to identify signs of corruption.

The article deals with the problem of violation of anti-corruption legislation in state and municipal institutions from the point of view of the psycho-emotional state of officials. It is proposed to use machine learning methods to analyze video and audio recordings of speeches with unprepared speech of officials of various levels of government, where they answer questions from journalists and the public, in order to determine emotions and identify aggression, uncertainty, and evasiveness in answers. The results of the study may be useful for government agencies involved in the fight against corruption, as well as for the public interested in transparency and honesty of the activities of civil servants.
Keywords: anti–corruption; public administration; machine learning; verbal analysis; analysis of audio-video recordings; analysis of psycho-emotional state
For citation: Krainovskikh V.I., Komarova A.A., Basov O.O. The method of identifying indirect signs of corruption acts based on video recordings of speeches of civil servants // Research result. Information technologies. – T.8, №2, 2023. – P. 35-45. DOI: 10.18413/2518-1092-2022-8-2-0-5

ВВЕДЕНИЕ

Проблема коррупции остается одной из самых актуальных в мире, и Россия не является исключением. По данным МВД России, только за первые шесть месяцев 2022 года число коррупционных преступлений в России увеличилось на 9,2% по сравнению с предыдущим годом [25]. К таким нарушениям относятся получение взяток, злоупотребление должностным положением и другие незаконные способы обогащения государственных служащих.

Коррупция является неотъемлемой частью системы теневой экономики, которая уменьшает доходы государства. В результате многие экономические транзакции происходят вне официальной экономики и не облагаются налогами. Международный Валютный Фонд оценивает потери мировой экономики от коррупции от 1,5 трлн. до 2 трлн. долларов ежегодно [24]. Кроме того, коррупционные последствия могут быть катастрофическими для экономического и социального развития страны. Они искажают нормы морали и подрывают авторитет государственной власти в глазах граждан. Однако, несмотря на все эти негативные последствия, коррупция продолжает существовать во многих странах, и борьба с ней остается одной из важнейших задач в области государственного управления.

Хоть данный феномен и является трудно наблюдаемым, однако сегодня все больше стран стараются пресечь коррупционные деяния путем внедрения современных информационных технологий. Россия не стала исключением и также рассматривает искусственный интеллект как вариант профилактики коррупционных действий [26]. На сегодняшний день применяются информационно–коммуникационные технологии, связанные с формированием транспарентности органов публичной власти. Такими примерами могут служить электронные порталы, на которых государственные служащие могут обнародовать свои доходы и имущество, онлайн-реестры государственных закупок, системы электронного документооборота и даже приложения для мобильных устройств, позволяющие гражданам сообщать о коррупционных проявлениях. Однако, применение технологий не является панацеей от коррупции и не гарантирует полное ее исключение.

Существует связь между определенными языковыми, поведенческими и невербальными проявлениями на аудио–видеозаписях и совершением коррупционных деяний. Например, наличие специфических лингвистических выражений, сигналов и жестов, которые могут указывать на протекцию, взяточничество, подкуп или другие формы коррупции. Данная гипотеза предполагает, что во время совершения коррупционных деяний люди могут проявлять определенное поведение, использовать специфическую лексику, жестикуляцию или другие невербальные средства, которые могут быть записаны на аудио–видеозаписях. Анализ этих записей может помочь выявить определенные признаки, которые указывают на возможное совершение коррупционных деяний.

Анализ видео и аудио записей с выступлениями чиновников, в которых они отвечают на вопросы журналистов и общественности, может стать эффективным инструментом в борьбе с коррупцией. Такой анализ ответов помогает определять степень уклончивости, неуверенности и агрессии государственных служащих, что может навести на следы коррупционных деяний. Связь

этих характеристик с реальными нарушениями антикоррупционного законодательства может дать более полное представление об уровне коррупции в государственных и муниципальных учреждениях и помочь в разработке эффективных стратегий борьбы с данной проблемой, и в дальнейшем может обеспечить прозрачность и честность в работе государственных и муниципальных учреждений в будущем.

Данная работа направлена на разработку метода выявления признаков нарушения антикоррупционного законодательства в видеозаписях выступлений госслужащих, основанного на определении таких косвенных признаков как неуверенность, наличие агрессии и уклончивость в ответах госслужащих при анализе уровня коррупции в государственных и муниципальных учреждениях.

ОСНОВНАЯ ЧАСТЬ

В рамках данного исследования была принята гипотеза о наличии взаимосвязи между тремя психоэмоциональными характеристиками, которые может проявлять человек в случаях нарушения антикоррупционного законодательства: агрессия, неуверенность и уклончивость в ответах. Был проведен сбор данных, состоящий из видео выступлений чиновников разного уровня власти, для определения поведенческих маркеров трех психоэмоциональных характеристик.

Методика выявления признаков нарушения антикоррупционного законодательства в видеозаписях чиновников состоит из трех модулей: детекции агрессии, неуверенности и уклончивости в ответах, и основана на анализе видеоматериалов с неподготовленной речью чиновника. На вход подается видеоматериал, из которого извлекаются видео и аудио каналы. Аудиоканал подвергается процессу транскрибации, для получения текстового значения выступления. После чего необходимые потоки данных подаются на вход трем модулям для дальнейшего анализа. Структура разрабатываемого метода представлена на Рисунке 1:

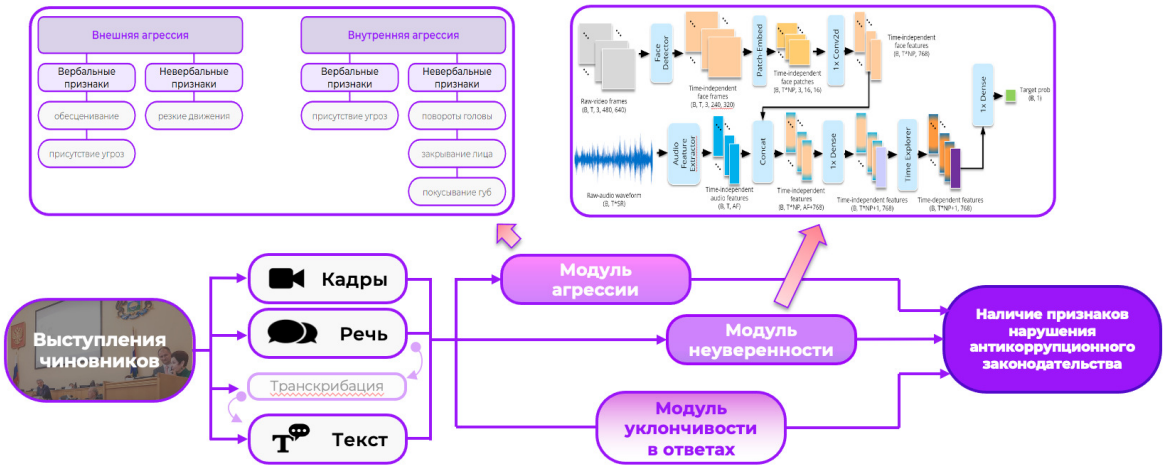

Рис. 1. Структура разрабатываемого метода выявления косвенных признаков нарушения антикоррупционного законодательства в видеозаписях выступлений госслужащих

Fig. 1. Structure of the developed method for identifying indirect signs of violation of anti-corruption legislation in video recordings of speeches of civil servants

Выборка данных состоит из различных видео материалов с неподготовленной речью чиновников различного уровня, где они отвечают на различные вопросы: записи встреч и переговоров с представителями бизнеса, СМИ и общественностью, а также записи ответов на вопросы, связанных с их должностью, доходом и коррупционными действиями. Схема с классификацией используемых ресурсов с неподготовленной речью чиновников представлена на рисунке 2:

Рис. 2. Схема с используемыми ресурсами неподготовленной речи чиновников
Fig. 2. A diagram with the resources used for the unprepared speech of officials

На Рисунке 3 представлена классификация вопросов, которые используются в дальнейшем анализе видеофрагментов из выступлений госслужащих:

Характеристики вопросов

Категория вопросов	Описание
Финансовые вопросы	Относятся к финансовым аспектам деятельности и могут выявлять наличие взяточничества, рассекречивания, отмывания денег и других финансовых махинаций
Контакты с лицами, связанными с коррупцией	Относятся к общению и взаимодействию с лицами,связанными с коррупцией, такими как чиновники, представители частных компаний и т.д.
Использование влияния и ресурсов	Относятся к использованию личного или служебного влияния и ресурсов в корыстных целях, в том числе использование служебного положения или ресурсов для получения личной выгоды
Запросы на взятки и неправомерные выгоды	Относятся к прямому запросу на получение денежных средств, подарков или других неправомерных выгод в обмен на предоставление услуг
•••	•••

Рис. 3. Рассматриваемые категории вопросов, задающиеся чиновникам
Fig. 3. Considered categories of questions asked to officials

Для дальнейшего анализа требуется, чтобы каждый фрагмент записей описывался набором невербальных и вербальных маркеров поведения. Ниже представлены методы, использующиеся для извлечения указанных маркеров.

ДЕТЕКЦИЯ АГРЕССИИ

Данный модуль позволяет определить степень агрессии говорящего. Сперва уточним, что подразумевается под агрессией: агрессия – это поведение, целью которого является причинение вреда объекту нападения (будь то живое существо или неодушевленный предмет), оно несовместимо с общепринятыми нормами и правилами поведения в обществе; проявлением такого поведения может быть как физический ущерб, так и вызванные негативные эмоции или психологический дискомфорт у объекта нападения (чувство страха, беспокойства, тревоги, депрессии и т. д.) [2].

Агрессию лучше всего рассматривать с точки зрения двух характеристик: внутреннего и внешнего проявления. Для определения агрессии следует учитывать вербальные и невербальные сигналы, они разделяются следующим образом:

Невербальные сигналы:

- темп речи;
- резкое повышение/понижение громкости речи;
- эмоциональный окрас речи: злость, отвращение, спокойствие, радость, страх, удивление, печаль.

Вербальные сигналы:

- наличие повелительного наклонения;
- наличие нецензурной лексики и жаргона в тексте;
- наличие уменьшительно-ласкательных\уменьшительно-унизительных конструкций;
- наличие оскорблений;
- наличие угроз;
- наличие токсичности.

Токсичность в высказываниях описывается как качество высказывания, которое проявляется в язвительных, агрессивных, оскорбительных, унижающих или провоцирующих высказываниях, которые могут вызвать негативные эмоции, оскорбить, унизить или причинить вред другому человеку или группе людей.

Набор данных содержал записи с выступлений чиновников, на которых присутствовали посторонние шумы, разговоры других людей и т.д. Поэтому перед анализом данных было необходимо провести предварительную обработку, включающую удаление шумов и нормализацию громкости [14].

Темп речи измеряется в количестве произнесенных слов в минуту. Для вычисления этого показателя используется спектральный поток сигнала, который вычисляется с помощью функций из библиотеки «Librosa» [15]. Затем производится подсчет количества пиковых значений, которые считаются началом каждого слова.

Для определения "резкого" изменения громкости применяется эвристический метод, заключающийся в измерении угла наклона между соседними отсчетами амплитудной огибающей и абсолютным расстоянием до максимального значения. Если амплитудное значение отсчета близко к максимальному значению по всей записи и изменение происходит быстрее, чем переход к другим значениям внутри записи, то это изменение громкости считается "резким".

Для определения класса эмоций была обучена сверточная нейронная сеть с полносвязным классификатором, аудио–сигнал в которой представлен в виде мел-кепстральных коэффициентов, подающиеся на вход сети [8]. Для того, чтобы в ходе обучения не возникло ситуации переобучения на одном языке [11], были выбраны следующие наборы данных: CaFE [9], Emo-DB [5], RAVDESS [13], SAVEE [17]. В полученный набор были включены короткие аудиозаписи, отнесенные к одному из семи классов эмоций, которые соотносятся с классификацией эмоций Р. Вудвортста [1]: злость, скука, тревога, радость, печаль, отвращение и нейтральное состояние (отсутствие эмоции). Для классификации эмоций используется фрагмент длительностью 3 секунды, а в случае, если он имеет меньшую длительность, его заполняют нулями до необходимого размера.

Для оценки вербальных признаков, подающихся из текста, необходимо было провести процедуру транскрибации речи. С этой целью, был выбран набор инструментов Vosk.

Был собран словарь из 140 тыс. слов, состоящий из максимально всевозможных морфологических вариантов слов нецензурной лексики, с целью ее детектирования из речи. Каждое слово входящего текста проверяется по данному словарю и подсчитывается количество нецензурной лексики в тексте.

Для детекции слов, находящихся в повелительном наклонении, была использована библиотека pymorphy2, с помощью которой возможен полный морфологический разбор слова [10].

Для детекции уменьшительно-ласкательных и пренебрежительных выражений, окончания слов были отброшены с использованием стеммера (процесс нахождения основы слова) Портера, адаптированного для русского языка. Далее была проверка на наличие уменьшительно-

ласкательных суффиксов у слова, включая все возможные морфологические варианты, такие как "ик", "ек", "к", "ец", "иц", "оск", "ечк", "оньк", "еньк", "ышк", "инш", "ушк" и "юшк".

Обнаружение оскорблений и угроз в тексте было выполнено дообучение моделей бинарной классификации [3] с помощью нейронной сети, на базе архитектуры RuBertTiny [20].

Для детекции угроз:

- тесты, содержащие угрозу;
- тексты, не содержащие угроз.

Для детекции оскорблений:

- тексты, содержащие оскорбления;
- тексты, не содержащие оскорбления.

С помощью данных из социальной сети «Одноклассники» были взяты 248290 комментария, относящиеся к трем категориям: нейтральные сообщения, сообщения с оскорблениями и сообщения с угрозами.

Также была обучена модель RuBertTiny для детекции токсичности в речи [17]. Текст, содержащий дискриминирующие и оскорбительные сообщения по отношению к кому–либо, принято считать токсичным. Была обучена модель классификации на нескольких различных наборов данных [7].

ДЕТЕКЦИЯ НЕУВЕРЕННОСТИ

Данный модуль предназначен для того, чтобы понять степень уверенности говорящего. Уверенность формируется на основе успешного решения социальных задач и достижения поставленных целей.

Анализ данной характеристики будет проходить по двум сигналам: вербальным и невербальным. В каждом из них были выделены следующие показатели:

Невербальные сигналы:

- темп речи;
- резкое повышение/понижение громкости речи;
- эмоциональный окрас речи: радость, злость, нейтральное состояние.

Вербальные сигналы:

- содержание речи

Модуль работает с входными видеозаписями чиновников, в ходе чего из них извлекаются последовательности из кадров и сэмплов длительностью 10 секунд для дальнейшего анализа. В работе модуля используется нейронная сеть–трансоффрмер (Рисунок 4) [19], с целью обработки мультимодального потока видео [22, 21, 23].

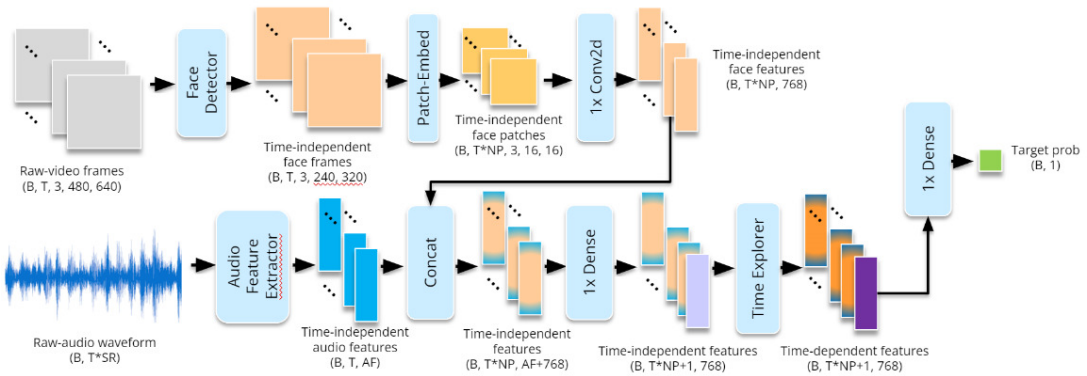

Рис. 4. Пайплайн определения уверенности человека с помощью сети-трансформер
Fig. 4. Pipeline for determining a person's confidence using a transformer network

Существует два способа, чтобы произвести извлечение необходимых признаком как из видеоматериалов, так и из аудиосигналов. Рассмотрим каждый более подробно, начнем с видеосигналов:

1) Для получения вектора мимики лица рассматриваемого человека используется сверточная нейронная сеть BlazeFace вместе с модулем Face Mesh [4], который извлекает вектор из 478 точек лица. Сеть принимает на вход изображение кадра видеопоследовательности в тензорном представлении, сжатом до 256x256 пикселей.

2) В альтернативном сценарии вместо точек лица используются более высокоуровневые признаки, полученные непосредственно из изображения лица человека реального размера, которое в дальнейшем векторизуется с помощью сверточной нейронной сети TinaFace.

Теперь рассмотрим существующие сценарии для извлечения признаков из аудиосигнала:

1) Извлечение интерпретируемых атрибутов из аудиопотока, таких как эмоции, дрожание голоса, тон, частота, амплитуда, количество и длительность пауз.

2) Преобразование аудиопотока в спектрограмму, по которой вычисляются MFCC коэффициенты [16, 6].

Следующим этапом является объединение аудио и видео сигналов в один поток мультимодальных признаков, основываясь на соответствующей их размерности [12]. Затем, к получившемуся потоку добавляется обучаемый вектор, и они вместе передаются в сеть-трансформер для обучения относительно временной размерности.

Модель содержит два нейрона с функцией активации сигмоид, которые предоставляют информацию о видеофрагменте:

1) Первый нейрон: происходит вычисление вероятности отнесения видеофрагмента к классу 0, что является оценкой уверенности в данной классификации;

2) Второй нейрон: происходит вычисление вероятности отнесения видеофрагмента к классу 1, что является оценкой неуверенности в данной классификации.

Согласно формулам, которые изображены ниже, происходит объединение результатов предсказаний для видеозаписей:

$$T = \frac{1}{n} * \sum_{i=0}^{1} \left(\frac{T_i}{T_i + F_i}\right),$$
$$F = \frac{1}{n} * \sum_{i=0}^{1} \left(\frac{F_i}{F_i + T_i}\right).$$

где T - значение уверенности первого нейрона (уверенность в высказывании);

F - значение уверенности второго нейрона (неуверенность в высказывании);

n - количество видеофрагментов в видео.

Эта формула позволяет оценить вклад каждого нейрона в предсказание модели, вместо того чтобы рассчитывать независимую оценку уверенности каждого нейрона:

– Значение в пределах 50% соответствует низкой степени уверенности эксперта.

– Значения от 50% до 70% соответствуют средней степени уверенности эксперта.

– Значения, превышающие 70%, соответствует более высокой степени уверенности.

ДЕТЕКЦИЯ УКЛОНЧИВОСТИ В ОТВЕТАХ

Уклончивость в ответах означает избегание прямых, ясных и конкретных ответов на вопросы или ведение обсуждения в сторону или избегание точного ответа на вопросы. Это может проявляться в использовании общих или неопределенных формулировок, уходе от прямых ответов, в различных альтернативах или отвлеченных рассуждениях, вмешательстве в детали или недостаточном предоставлении информации. Анализ научной литературы по данной теме позволило выделить и классифицировать наиболее распространенные способы избегания ответов.

Проанализировав ряд источников, была разработана схема на рисунке 5, в которой представлены различные способы уклончивости в ответах. В данной схеме визуализированы типичные приемы, которыми спикеры могут избегать прямых и конкретных ответов на вопросы. Классификация способов уклончивости включает такие категории, как ответ вопросом на вопрос, сомнение в задаваемом вопросе, отказ от ответа или игнорирование вопроса, и неполный ответ.

Рис. 5. Схема со способами избегания ответа на вопрос
Fig. 5. A diagram with ways to avoid answering the question

Разрабатываемый алгоритм выявления уклончивости в ответах представляет собой сложную систему, основанную на двух обученных моделях, представляет собой обобщенный подход, который может использоваться для анализа диалогов или речи спикера.

Первая модель, использующая трансформер BERT, выполняет классификацию вопросительных и утвердительных предложений [27]. Для дообучения этой модели был использован датасет, состоящий из около 81 тысячи утвердительных предложений из датасета SPAADIA и 131 тысячи вопросительных предложений из датасета SQuaD. В результате тестирования, данная модель показала высокое значение F-меры, составляющей 0.96 для вопросительных предложений, что в данном случае свидетельствует о ее эффективности.

Далее, ответ человека в качестве контекста передается во вторую модель, которая в свою очередь с определенной степенью уверенности выделяет этот ответ из речи. Эта модель была построена с использованием техники fine-tuning на основе трансформера RoBERTa. Данная архитектура RoBERTa аналогична архитектуре BERT, однако отличается подходом к обучению модели. RoBERTa использует увеличенный корпус для обучения и генерацию динамических mask-токенов, что способствует ее более точному обучению. В качестве датасета для дообучения данной модели был выбран SQuaD датасет, содержащий вопросы и ответы на них. Значение F1-меры для дообученной модели составило 0.83, что указывает на ее высокую производительность и способность выделять ответы на вопросы из контекста речи спикера.

Можно предположить, что при слишком высокой уверенности модели ее ответы будут чрезмерно категоричными и необходимо будет учитывать возможность ложных срабатываний. С другой стороны, при слишком низкой уверенности модели ответы будут неопределенными и непригодными для использования. Поэтому для достижения наилучших результатов важно подобрать оптимальную границу значения уверенности, при которой модель будет давать наиболее точные и пригодные для использования ответы. Эта граница была определена экспериментально, путем анализа результатов работы модели при разных значениях уверенности и выбора наилучшего значения на основе полученных данных.

Выходом разрабатываемого алгоритма являются списки с вопросами/ответами для каждого спикера, сопровождающиеся метками "уклончивый" или "не уклончивый", а также значениями уверенности модели. Для каждого вопроса/ответа алгоритм определяет, является ли он уклончивым или нет, на основе выводов первой модели, осуществляющей классификацию предложений. Значение уверенности модели также возвращается в виде числовой оценки, отражающей степень уверенности алгоритма в своих выводах.

Таким образом, данная обобщенная модель, состоящая из двух шагов и двух обученных моделей, позволяет эффективно анализировать диалоги или речь спикера, классифицировать предложения и выделять ответы на вопросы из контекста, открывая новые возможности для автоматического анализа и обработки естественного языка.

ЗАКЛЮЧЕНИЕ

В исследовании был предложен метод выявления косвенных признаков нарушения антикоррупционного законодательства на основе анализа видеозаписей выступлений чиновников. Данный метод предполагает использование единого использования трех модулей: детекции

агрессии, неуверенности и уклончивости при ответах, для автоматического анализа видеоматериалов и выявления потенциальных нарушений антикоррупционных норм.

Разработанный метод основывается на анализе различных признаков, таких как жесты, мимика, тон голоса, паузы и другие невербальные элементы выступлений. Эти признаки могут свидетельствовать о потенциальных нарушениях антикоррупционных законов, таких как неправдивые заявления, скрытые сделки, взяточничество и другие формы коррупционной деятельности.

Комбинируя результаты этих трех модулей, можно получить информацию о возможных нарушениях антикоррупционных норм и оценить степень риска. Такой подход позволяет существенно ускорить процесс обнаружения потенциальных нарушений и улучшить эффективность мониторинга коррупционных проявлений в государственных органах.

Однако стоит отметить, что разработанный метод является предварительным инструментом и не может служить основой для однозначного заключения о наличии или отсутствии нарушений. Для более точной оценки необходимо проводить дополнительные исследования, включая анализ сторонних источников информации и проверку результатов метода на большом объеме видеоматериалов с различными контекстами и условиями.

Список литературы

1. Овсянникова В. В. К вопросу о классификации эмоций: категориальный и многомерный подходы // Финансовая аналитика: проблемы и решения. – 2013. – №. 37. – С. 43-48.
2. Рогов Е. И. Настольная книга практического психолога: Учебное пособие // М.: ВЛАДОС. – 1998. – С. 134-142.
3. Самигулин Т. Р., Смирнов И. З., Лаушкина А. А. Определение маркеров агрессивного поведения человека на основе анализа аудио и текстового каналов // Научный результат. Информационные технологии. – 2022. – Т. 7. – №. 2. – С. 55-62.
4. Bazarevsky V. et al. Blazeface: Sub-millisecond neural face detection on mobile gpus //arXiv preprint arXiv:1907.05047. – 2019.
5. Burkhardt F. et al. A database of German emotional speech // Interspeech. – 2005. – Т. 5. – С. 1517-1520.
6. Chow A., Louie J. Detecting lies via speech patterns. – 2017.
7. Devyatkin D. A. et al. Intelligent analysis of manifestations of verbal aggressiveness in network community texts //Scientific and Technical Information Processing. – 2014. – Т. 41. – С. 377-389.
8. Goupil L. et al. Listeners' perceptions of the certainty and honesty of a speaker are associated with a common prosodic signature // Nature communication. – 2021. – Т. 12. – №. 1. – С. 861.
9. Gournay P., Lahaie O., Lefebvre R. A canadian french emotional speech dataset //Proceedings of the 9th ACM multimedia systems conference. – 2018. – С. 399-402.
10. Korobov M. Morphological analyzer and generator for Russian and Ukrainian languages //Analysis of Images, Social Networks and Texts: 4th International Conference, AIST 2015, Yekaterinburg, Russia, April 9–11, 2015, Revised Selected Papers 4. – Springer International Publishing, 2015. – С. 320-332.
11. Kossaifi J. et al. Sewa db: A rich database for audio-visual emotion and sentiment research in the wild // IEEE transactions on pattern analysis and machine intelligence. – 2019. – Т. 43. – №. 3. – С. 1022-1040.
12. Laushkina, Anastasia & Smirnov, Ivan & Medvedev, Anatoly & Laptev, Andrey & Sinko, Mikhail. (2022). Detecting incongruity in the expression of emotions in short videos based on a multimodal approach. Cybernetics and Physics. 210-216.
13. Luna-Jiménez C. et al. A Proposal for Multimodal Emotion Recognition Using Aural Transformers and Action Units on RAVDESS Dataset // Applied Sciences. 2021. – Vol. 12. – № 1. – P. 327.
14. Marcolla F., de Santiago R., Dazzi R. Novel Lie Speech Classification by using Voice Stress // Proceedings of the 12th International Conference on Agents and Artificial Intelligence. SCITEPRESS – Science and Technology Publications. – 2020. – С. 742–749.
15. McFee B. et al. librosa: Audio and music signal analysis in python //Proceedings of the 14th python in science conference. – 2015. – Т. 8. – С. 18-25.
16. Oviatt S. et al. (ed.). The Handbook of Multimodal-Multisensor Interfaces: Signal Processing, Architectures, and Detection of Emotion and Cognition-Volume 2. – Association for Computing Machinery and Morgan & Claypool, 2018.

17. S. Haq P.J.B.J. Multimodal Emotion Recognition / ed. Wang W. IGI Global, 2010. C. 398–423.
18. Saeed H. H., Shahzad K., Kamiran F. Overlapping toxic sentiment classification using deep neural architectures //2018 IEEE international conference on data mining workshops (ICDMW). – IEEE, 2018. – С. 1361-1366.
19. Sinko M. et al. Method of constructing and identifying predictive models of human behavior based on information models of non-verbal signals //Procedia Computer Science. – 2022. – Т. 212. – С. 171-180.
20. Tenney I., Das D., Pavlick E. BERT rediscovers the classical NLP pipeline // arXiv preprint arXiv:1905.05950. – 2019.
21. Tsai Y. H. H. et al. Learning factorized multimodal representations // arXiv preprint arXiv:1806.06176. – 2018.
22. Tsai Y. H. H. et al. Multimodal transformer for unaligned multimodal language sequences //Proceedings of the conference. Association for Computational Linguistics. Meeting. – NIH Public Access, 2019. – Т. 2019. – С. 6558.
23. Tzirakis P. et al. End-to-end multimodal emotion recognition using deep neural networks //IEEE Journal of selected topics in signal processing. – 2017. – Т. 11. – №. 8. – С. 1301-1309.
24. В МВФ оценили потери мировой экономике от коррупции [Электронный ресурс]. – Режим доступа: https://www.rbc.ru/economics/18/09/2017/59bfead89a794704d063c4f0 (дата обращения: 03.04.2023).
25. Краткая характеристика состояния преступности в Российской Федерации за январь-июнь 2022 года. URL: https://xn--b1aew.xn--p1ai/reports/item/31209853/ (дата обращения: 03.04.2023).
26. НИУ ВШЭ предложил использовать искусственный интеллект для предотвращения коррупции в РФ [Электронный ресурс]. – Режим доступа: https://tass.ru/ekonomika/14304599 (дата обращения: 03.04.2023).
27. Bert for Sequence Classification (Question vs Statement)_ [Электронный ресурс]. – Режим доступа: https://sparknlp.org/2021/11/04/bert_sequence_classifier_question_statement_en.html (дата обращения: 15.04.2023).

References

1. Ovsyannikova V.V. On the question of the classification of emotions: categorical and multidimensional approaches // Financial analytics: problems and solutions. – 2013. – No. 37. – P. 43-48.
2. Rogov E.I. The handbook of a practical psychologist: a textbook //Moscow: VL. – 1998. – P. 134-142.
3. Samigullin T.R., Smirnov I.Z., Laushkina A.A. Determination of markers of aggressive human behavior based on the analysis of audio and text channels //Scientific result. Information technology. – 2022. – Vol. 7. – No. 2. – P. 55-62.
4. Bazarevsky V. et al. Blazeface: Sub-millisecond neural face detection on mobile gpus //arXiv preprint arXiv:1907.05047. – 2019.
5. Burkhardt F. et al. A database of German emotional speech // Interspeech. – 2005. – T. 5. – P. 1517-1520.
6. Chow A., Louie J. Detecting lies via speech patterns. – 2017.
7. Devyatkin D. A. et al. Intelligent analysis of manifestations of verbal aggressiveness in network community texts //Scientific and Technical Information Processing. – 2014. – T. 41. – P. 377-389.
8. Goupil L. et al. Listeners' perceptions of the certainty and honesty of a speaker are associated with a common prosodic signature // Nature communication. – 2021. – T. 12. – №. 1. – P. 861.
9. Gournay P., Lahaie O., Lefebvre R. A canadian french emotional speech dataset // Proceedings of the 9th ACM multimedia systems conference. – 2018. – P. 399-402.
10. Korobov M. Morphological analyzer and generator for Russian and Ukrainian languages // Analysis of Images, Social Networks and Texts: 4th International Conference, AIST 2015, Yekaterinburg, Russia, April 9–11, 2015, Revised Selected Papers 4. – Springer International Publishing, 2015. – P. 320-332.
11. Kossaifi J. et al. Sewa db: A rich database for audio-visual emotion and sentiment research in the wild // IEEE transactions on pattern analysis and machine intelligence. – 2019. – T. 43. – №. 3. – P. 1022-1040.
12. Laushkina, Anastasia & Smirnov, Ivan & Medvedev, Anatoly & Laptev, Andrey & Sinko, Mikhail. (2022). Detecting incongruity in the expression of emotions in short videos based on a multimodal approach. Cybernetics and Physics. P. 210-216.
13. Luna-Jiménez C. et al. A Proposal for Multimodal Emotion Recognition Using Aural Transformers and Action Units on RAVDESS Dataset // Applied Sciences. 2021. – Vol. 12. – № 1. – P. 327.
14. Marcolla F., de Santiago R., Dazzi R. Novel Lie Speech Classification by using Voice Stress // Proceedings of the 12th International Conference on Agents and Artificial Intelligence. SCITEPRESS – Science and Technology Publications. – 2020. – P. 742–749.

15. McFee B. et al. librosa: Audio and music signal analysis in python //Proceedings of the 14th python in science conference. – 2015. – T. 8. – P. 18-25.
16. Oviatt S. et al. (ed.). The Handbook of Multimodal-Multisensor Interfaces: Signal Processing, Architectures, and Detection of Emotion and Cognition-Volume 2. – Association for Computing Machinery and Morgan & Claypool, 2018.
17. S. Haq P.J.B.J. Multimodal Emotion Recognition / ed. Wang W. IGI Global, 2010. P. 398–423.
18. Saeed H. H., Shahzad K., Kamiran F. Overlapping toxic sentiment classification using deep neural architectures //2018 IEEE international conference on data mining workshops (ICDMW). – IEEE, 2018. – P. 1361-1366.
19. Sinko M. et al. Method of constructing and identifying predictive models of human behavior based on information models of non-verbal signals //Procedia Computer Science. – 2022. – T. 212. – P. 171-180.
20. Tenney I., Das D., Pavlick E. BERT rediscovers the classical NLP pipeline // arXiv preprint arXiv:1905.05950. – 2019.
21. Tsai Y. H. H. et al. Learning factorized multimodal representations // arXiv preprint arXiv:1806.06176. – 2018.
22. Tsai Y. H. H. et al. Multimodal transformer for unaligned multimodal language sequences //Proceedings of the conference. Association for Computational Linguistics. Meeting. – NIH Public Access, 2019. – T. 2019. – P. 6558.
23. Tzirakis P. et al. End-to-end multimodal emotion recognition using deep neural networks // IEEE Journal of selected topics in signal processing. – 2017. – T. 11. – №. 8. – P. 1301-1309.
24. The IMF estimated the losses to the world economy from corruption [Electronic resource]. – URL: https://www.rbc.ru/economics/18/09/2017/59bfead89a794704d063c4f0 (date of application: 03.04.2023).
25. Brief description of the state of crime in the Russian Federation for January-June 2022. URL: https://xn--b1aew.xn--p1ai/reports/item/31209853 / (accessed 03.04.2023).
26. HSE has proposed using artificial intelligence to prevent corruption in the Russian Federation [Electronic resource]. – URL: https://tass.ru/ekonomika/14304599 (date of application: 03.04.2023).
27. Bert for Sequence Classification (Question vs Statement) [Electronic resource]. – URL: https://sparknlp.org/2021/11/04/bert_sequence_classifier_question_statement_en.html (accessed: 04/15/2023).

Крайновских Вероника Игоревна, студент 4–го курса бакалавриата
Комарова Алёна Алексеевна, магистрант факультета цифровой трансформации
Басов Олег Олегович, доктор технических наук, доцент, профессор факультета цифровой трансформации

Krainovskikh Veronika Igorevna, 4th year Bachelor's student
Komarova Alyona Alekseevna, Master's student of the Faculty of Digital Transformation
Oleg Basov Olegovich, Doctor of Technical Sciences, Associate Professor, Professor of the Faculty of Digital Transformation

УДК 004.94 **DOI: 10.18413/2518-1092-2022-8-2-0-6**

Баскакова В.В.[1]
Жихарев А.Г.[2]

К ВОПРОСУ ПРИМЕНЕНИЯ СИСТЕМНО-ОБЪЕКТНОГО ИМИТАЦИОННОГО МОДЕЛИРОВАНИЯ ОРГАНИЗАЦИОННО-ДЕЛОВЫХ ПРОЦЕССОВ

[1)] Белгородский государственный национальный исследовательский университет, ул. победы, 85, Белгород, 308015, Россия
[2)] Белгородский государственный технологический университет им. В.Г. Шухова, ул. Костюкова, 46, Белгород, 308012, Россия

e-mail: baskakova_vv@bsaa.edu.ru, zhikharev@bsu.edu.ru

Аннотация
Осуществление имитационного моделирования управленческих процессов – это один из самых эффективных методов поддержки принятия решений, что доказано опытом использования подобных инструментов. Цель данной статьи определена в необходимости описать процедуру реализации системно-объектной имитационной модели распределения информации о студентах, учитывая структурные подразделения в высшем учебном заведении. В ходе исследования был сделан вывод, что благодаря применению методов имитационного моделирования в управленческой деятельности возможно существенным образом повысить эффективность управления деятельностью ВУЗа, выбрать перспективные направления ее развития.
Ключевые слова: абитуриент; контингент ВУЗа; приемная комиссия; процесс; моделирование; имитационная модель; системы проектирования
Для цитирования: Баскакова В.В., Жихарев А.Г. К вопросу применения системно-объектного имитационного моделирования организационно-деловых процессов // Научный результат. Информационные технологии. – Т.8, №2, 2023. – С. 46-52. DOI: 10.18413/2518-1092-2023-8-2-0-6

Baskakova V.V.[1]
Zhikharev A.G.[2]

TO THE QUESTION OF APPLICATION OF SYSTEM-OBJECT SIMULATION OF ORGANIZATIONAL AND BUSINESS PROCESSES

[1)] Belgorod State Technological University named after V.G. Shukhov, 46 Kostyukova St., Belgorod, 308012, Russia
[2)] Belgorod State National Research University, 85 Pobedy St., Belgorod, 308015, Russia
e-mail: baskakova_vv@bsaa.edu.ru, zhikharev@bsu.edu.ru

Abstract
The implementation of simulation modeling of management processes is one of the most effective methods of support. The purpose of this article is defined in the need to describe the procedure for implementing a system-object simulation model of the distribution of information about students, taking into account the structural units in a higher educational institution. In the course of the study, it was concluded that due to the use of simulation modeling methods in management activities, it is possible to significantly improve the efficiency of managing the university's activities and choose promising areas for its development.
Keywords: applicant; university contingent; admissions committee; process; modeling; simulation model; design systems
For citation: Baskakova V.V., Zhikharev A.G. To the question of application of system-object simulation of organizational and business processes // Research result. Information technologies. – T.8, №2, 2023. – P. 46-52. DOI: 10.18413/2518-1092-2022-8-2-0-6

ВВЕДЕНИЕ

В современной системе высшего образования, как и ранее, есть процессы, без которых не представляется возможным реализация учета контингента студентов. Данная работа акцентирует особое внимание на процесс ввода новых и учета имеющегося состава абитуриентов.

Актуальность работы заключается в постоянной необходимости ведения учета и пополнения в базах данных сведениях о контингенте в ВУЗах. Процесс обработки документов новых абитуриентов для текущей приемной комиссии имеет множество особенностей и вариантов развития. Деятельность приемной компании, тесно связана с проделанными в предыдущие периоды времени профориентационными мероприятиями.

Немаловажно учитывать формализованные изменения в требованиях к организационным процессам такого рода. Так, например, на современном этапе уже не представляется возможным деятельность образовательной организации без проведения, как внутренних мониторингов, так и сбора статистических данных, которые анализируются и предназначаются для внешних структур [4;37].

В работе особое внимание уделено процессу приема документов на поступление и зачисление абитуриентов в ряды студентов высшего учебного заведения. Этот процесс включает в себя большое количество составляющих, которые, в свою очередь, формально ограничиваются федеральными нормативно-правовыми актами в сфере образования.

Чтобы решить подобные организационные задачи требуется рациональным образом использовать процесс имитационного моделирования.

ОПИСАНИЕ ПРОЦЕССОВ ПРИЕМА АБИТУРИЕНТОВ

В данной работе рассматривается процесс приема абитуриентов и осуществление документооборота по вопросам приема в ВУЗах. В данном случае его рассматривают в качестве организационно-делового процесса.

Описывая процесс движения контингента ВУЗа необходимо начинать с процесса поступления студента. На этом этапе в работе будет сделан особый акцент.

Применен современный инструмент UFOModeler. Его суть связана с использованием CASE/BI-инструментария, который основан на знаниях. Программа используется в целях моделирования и проектирования сложных систем, в том числе организационных, информационных и технических. Основу инструмента составляет отечественный метод системного анализа (УФО-анализ), который обеспечивает представление системы в виде Узлов (структурная характеристика), Функций (динамическая характеристика) и Объектов (субстанциальная характеристика). УФО-анализ выступает в качестве первого метода системного анализа, который согласуется с объектно-ориентированным подходом.

Процесс приема документов у потенциального абитуриента описан в представленных схемах. Основная схематическая часть описывает «движение» самого абитуриента-студента (человек вне университета, но желающий стать студентом –абитуриент). Далее идет сам процесс подачи документов (со стороны абитуриента) и приема пакета документов (со стороны университета). Входными данными определяется особый пакет документов абитуриента (паспортные данные, СНИЛС, ИНН, уровень ранее полученного образования, документ об образовании, гражданство, при необходимости паспортные данные родителя (<18 лет), целевой договор и документы, подтверждающие отношение к льготной категории лиц (при наличии) [8; 5].

Вспомогательными позициями процесса приема абитуриента будут выступать ответственный и технические секретари. Управление процессом происходит на основе законодательных актов, в частности Положения "О правилах приема" и Приказа об утверждении правил приема.

Исходные данные процесса приема абитуриентов являются приказами на зачисление и списками добавленных в контингент ВУЗа.

Рис. 1. Основная схема процесса «Прием и зачисление»
Fig. 1. Basic scheme of the process "Admission and enrollment"

Более подробное рассмотрение процесса «Прием и зачисление» представлено на декомпозициях.

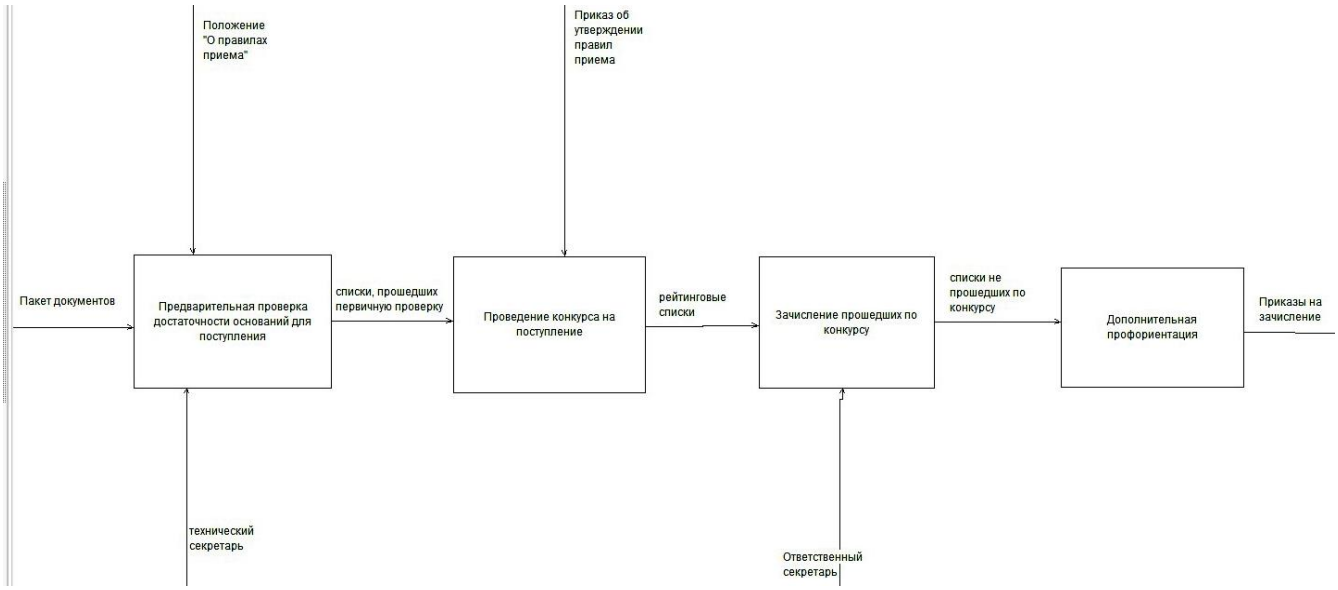

Рис. 2. Декомпозиция процесса «Прием и зачисление»
Fig. 2. Decomposition of the process "Admission and enrollment"

Данная схема показывает то, что процесс приема и зачисления студентов разбит на подпроцессы:

- предварительная проверка достаточности оснований для поступления;
- проведение конкурса на поступление;
- зачисление прошедших по конкурсу;
- дополнительная профориентация.

Естественно, что входящей информацией в декомпозиционные процессы является также, как и в основном процессе, пакет документов.

АНАЛИЗ СХЕМЫ ПРОЦЕССОВ «КОНКУРС НА ПОСТУПЛЕНИЕ», «ЗАЧИСЛЕНИЕ», «ДОПОЛНИТЕЛЬНЯ ПРОФОРИЕНТАЦИЯОННАЯ РАБОТА»

В свою очередь, у каждого подпроцесса есть составляющие его действия. Так, подпроцесс «Предварительная проверка достаточности оснований для поступления» состоит из первичного приема пакета документов, формирования электронного и личного дела абитуриента в бумажном виде, выделения категорий абитуриентов и списков по льготному основанию поступления.

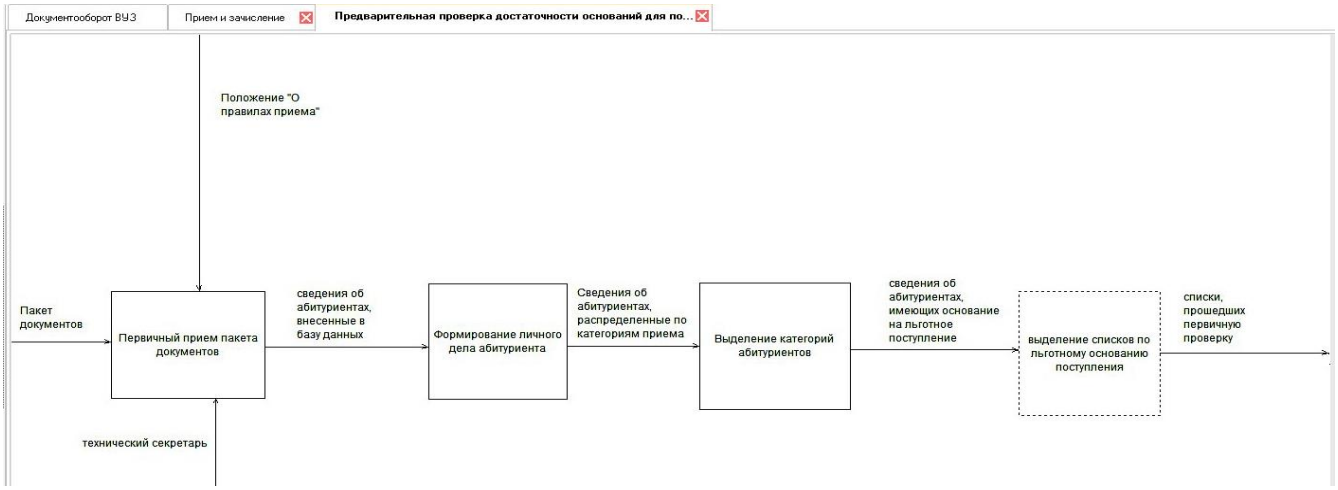

Рис. 3. Декомпозиция предварительной проверки достаточности оснований для поступления
Fig. 3. Decomposition of a preliminary check of the sufficiency of grounds for admission

Далее рассматриваются составляющие действия подпроцесса «Проведение конкурса на поступление».

Рис. 4. Декомпозиция проведения конкурса на поступление
Fig. 4. Decomposition of the competition for admission

В схеме входящими данными являются списки абитуриентов, которые прошли первичную проверку. На данном этапе проводится работа только с абитуриентами по общему бюджетному конкурсу. Льготные категории и абитуриенты с целевыми договорами на этом этапе уже не участвуют. В этой ситуации можно судить о двух основных потоках: поступающих на основании справки ЕГЭ и поступающих на основании оконченного среднего образования. Первый тип абитуриентов сдает документы и справку о сдаче ЕГЭ. Последняя автоматически выгружается в базу данных ВУЗа, а следом и на сайт с рейтинговым списком [5; 29]. Второй тип абитуриентов сдает внутренние испытания на базе ВУЗа и по итогам этих испытаний баллы также вносятся в рейтинговый общий список.

На рисунке 5, представленном ниже на схеме можно отследить движение рейтинговых списков по всем необходимым формальным пунктам, необходимым для выпуска приказа на зачисление.

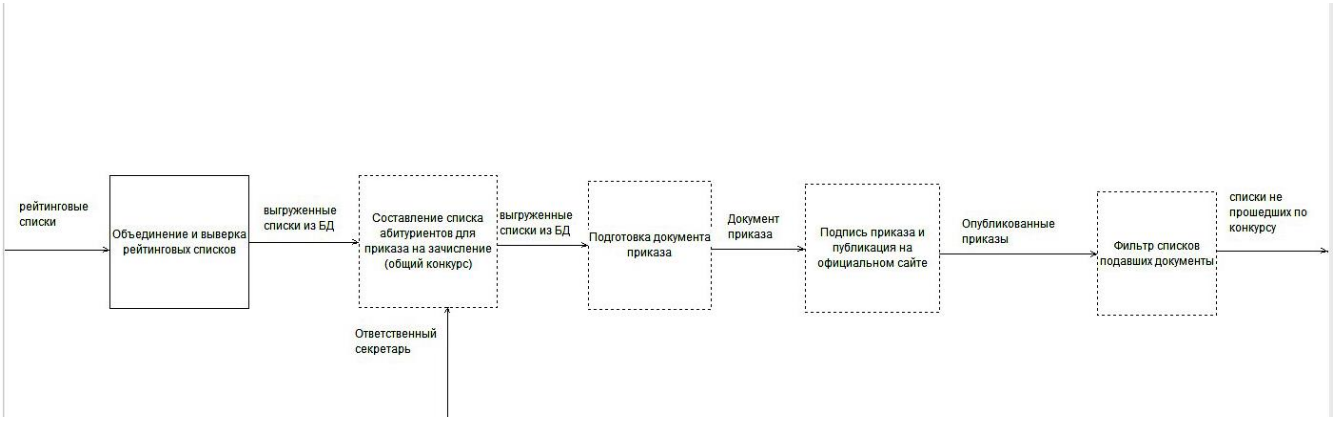

Рис. 5. Декомпозиция процесса зачисления прошедших по конкурсу
Fig. 5. Decomposition of the process of enrolling those who passed through the competition

В период проведения приемной кампании, в большинстве случаев, после зачисления льготных категорий, целевиков и тех, кто прошел по конкурсу на бюджетное место, остаются конкурсанты, которые не прошли на бюджет. С такими абитуриентами, предполагается проведение дополнительной профориентационной работы. Если конкурсант участвовал (по своему праву) в общем конкурсе, то им были пройдены нижние пороги по ЕГЭ и внутренние испытания. В случае его согласия, такой конкурсант может пройти на конкурс на коммерческие места.

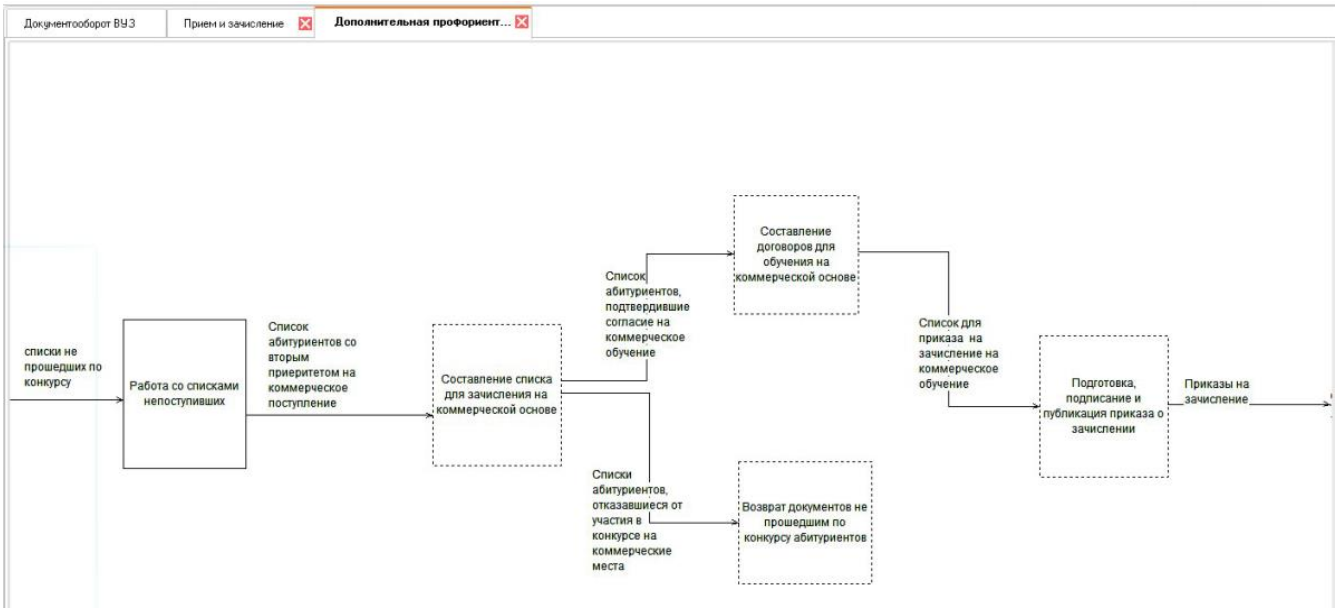

Рис. 6. Схема проведения дополнительной профориентационной работы после проведения процесса зачисления на бюджетные места
Fig. 6. Scheme for conducting additional career guidance work after the process of enrolling in budget places

В процессе подписания согласия на обучение, осуществляемого на платной основе, требуется составить договор на оказание платных образовательных услуг. В этом случае ему будет присвоен индивидуальный номер, проставлена дата заключения договора. Когда вносятся вышеуказанные данные, то осуществляется процесс по группировке абитуриентов, учитывая признак ранее полученного образования, выбранных направлений для обучения, сортировка в рейтинговых списках происходит с учетом среднего балла аттестата / сумме баллов по государственному экзамену (автоматически сортирует данные по признаку «средний балл по

аттестату» или «результаты вступительных испытаний» от большего значения к меньшему) [9; 43].

ЗАКЛЮЧЕНИЕ

Таким образом, имитационное моделирование выступает в качестве способа по учету максимально возможного числа факторов внешней среды. Именно они позволяют поддержать принятие верного управленческого решения.

Имитационное моделирование в таком случае является мощным инструментом по управлению проектами. В ходе развития специализированных программных средств и распространением информации о теоретических и практических вариантах осуществления моделирования, процесс создания имитационных моделей будет проходить проще.

В исследовании была рассмотрена процедура имитационного моделирования во время работы приемной комиссии. Для наглядности описания процесса были разработаны авторские схемы. Полученный результат имитационной модели можно дополнять разного рода анализами (в том числе вероятностными или статистическими). Таким образом, становится возможным облегчить и обеспечить бесперебойную работу приемной комиссии, получая полные данные по каждому абитуриенту.

Список литературы

1. Алиев Т.И. Основы моделирования дискретных систем. Учебное пособие. СПб.: СПбГУ ИТМО. 2009. 363 с.

2. Белайчук А.А., Елифёров В.Г., Свод знаний по управлению бизнес-процессами: BPM CBOK 3.0. М.: Альпина Паблишер. 2018. 480 с.

3. Громов А., Каменнова М., Старыгин А. Управление бизнес-процессами на основе технологии Workflow // Открытые системы. СУБД. 1997. №1. Режим доступа: https://www.osp.ru/os/1997/01/179063. (Дата обращения 05.03.2020).

4. Калинин А.Г. Обработка данных методами математической статистики. Чита: СибУПК. 2015. 106 с.

5. Калянов Г. Н. О теории бизнес-процессов // Программная инженерия. 2018. №9(3). С. 99-109. DOI: 10.17587/prin.9.99-108

6. Квартани Т., Палистрант Дж. Визуальное моделирование с помощью IBM Rational Software Architect и UML. Пер. сангл. М.: КУДИЦ-ПРЕСС. 2007. 192 с.

7. Митрофанова Е.А., Коновалова В.Г., Митрофанова А.Е. Технология определения и планирования потребности в персонале определенного профессионального уровня и компетенций // Проблемы управления и моделирования в сложных системах: Труды XXI Международной научной конференции. Самара: ООО «Офорт». 2019. Т. 2. С. 455-460.

8. Новичков А., Карабанова Г. Моделирование бизнес-процессов автоматизируемой предметной области при помощи диаграмм деятельности (Activitydiagram) с использованием RSA. [Электронный ресурс] // URL: http://www.ibm.com/developerworks/ru/library/r-rsa/index.html

9. Павловский Ю.Н., Белотелов Ю.Н., Бродский Ю.И. Имитационное моделирование. М.: Изд-во «Академия». 2008. 236 с.

References

1. Aliev T.I. Fundamentals of modeling discrete systems. Tutorial. St. Petersburg: SPbGU ITMO. 2009. 363 p.

2. Belaichuk A.A., Eliferov V.G., Body of knowledge on business process management: BPM CBOK 3.0. Moscow: Alpina Publisher. 2018. 480 p.

3. Gromov A., Kamennova M., Starygin A. Business process management based on Workflow technology. Open Systems. DBMS. 1997. No. 1. Access mode: https://www.osp.ru/os/1997/01/179063. (Accessed 05.03.2020).

4. Kalinin A.G. Data processing by methods of mathematical statistics. Chita: SibUPK. 2015. 106 p.

5. Kalyanov G. N. On the theory of business processes // Software engineering. 2018. No. 9(3). pp. 99-109. DOI: 10.17587/prin.9.99-108

6. Quartani T., Palistrant J. Visual modeling with IBM Rational Software Architect and UML. Per. English M.: KUDITS-PRESS. 2007. 192 p.

7. Mitrofanova E.A., Konovalova V.G., Mitrofanova A.E. Technology for determining and planning the need for personnel of a certain professional level and competencies // Problems of management and modeling in complex systems: Proceedings of the XXI International Scientific Conference. Samara: LLC "Etching". 2019. Vol. 2. P. 455-460.

8. Novichkov A., Karabanova G. Modeling business processes of an automated subject area using activity diagrams (Activitydiagram) using RSA. [Electronic resource] // URL: http://www.ibm.com/developerworks/ru/library/r-rsa/index.html

9. Pavlovsky Yu.N., Belotelov Yu.N., Brodsky Yu.I. Simulation modeling. Moscow: Academy Publishing House. 2008. 236 p.

Баскакова Валентина Валерьевна, аспирант кафедры информационных и робототехнических систем
Жихарев Александр Геннадиевич, доктор технических наук, доцент, доцент кафедры программного обеспечения вычислительной техники и автоматизированных систем

Baskakova Valentina Valerievna, postgraduate student of 4 years of Department of Information and Robotic Systems
Zhikharev Alexander Gennadievich, Doctor of Technical Sciences, Associate Professor, Associate Professor of the Department of Computer Engineering and Automated Systems Software

УДК 004.056 **DOI: 10.18413/2518-1092-2022-8-2-0-7**

Герасимов В.М. [1]
Маслова М.А. [2,3]
Халилаева Э.И. [2]

ЗАЩИТА ОТ СОСТЯЗАТЕЛЬНЫХ АТАК НА АУДИО И ИЗОБРАЖЕНИЯ В МОДЕЛЯХ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА С ПРИМЕНЕНИЕМ МЕТОДА SGEC

[1)] Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики», Кронверкский пр., д. 49, г. Санкт-Петербург, 197101, Россия
[2)] Севастопольский государственный университет, ул. Университетская, д. 33, г. Севастополь, 299053, Россия
[3)] Ростовский государственный экономический университет (РИНХ), ул. Большая Садовая, д. 69, 7. Ростов-на-Дону, 344002, Россия

e-mail: my.virus.kaspersky@gmail.com, mashechka-81@mail.ru, emine.halilaeva@yandex.ru

Аннотация
В современном мире использование искусственного интеллекта (ИИ) все чаще сталкивается с риском состязательных атак на аудио и изображения. Данная статья исследует эту проблему и представляет метод SGEC как средство минимизации этих рисков. Рассматриваются различные виды атак на аудио и изображения, такие как искажение разметки, атаки "белого ящика" и "черного ящика", утечки через обученные модели и атаки на уровне железа. Основной акцент делается на методе SGEC, который предлагает шифрование данных и обеспечение их целостности в моделях ИИ. Статья также рассматривает другие способы защиты аудио и изображений, включая двойную проверку и ансамбли методов, ограничение доступа и анонимизацию данных, а также использование доказуемо устойчивых моделей ИИ.
Ключевые слова: состязательные атаки; защита голосовых отпечатков; защита биометрических данных; стеганография; шифрование данных; риски состязательных атак
Для цитирования: Герасимов В.М., Маслова М.А., Халилаева Э.И. Защита от состязательных атак на аудио и изображения в моделях искусственного интеллекта с применением метода SGEC // Научный результат. Информационные технологии. – Т.8, №2, 2023. – С. 53-60. DOI: 10.18413/2518-1092-2022-8-2-0-7

Gerasimov V.M.[1]
Maslova M.A.[2,3]
Khalilayeva E.I. [2]

PROTECTION AGAINST ADVERSARIAL ATTACKS ON AUDIO AND IMAGES IN ARTIFICIAL INTELLIGENCE MODELS USING THE SGEC METHOD

[1)] Saint Petersburg National Research University of Information Technologies, Mechanics and Optics, 49 Kronverkskiy prospekt, St. Petersburg, 197101, Russia
[2)] Sevastopol State University, 33 Universitetskaya St., Sevastopol, 299053, Russia
[3)] Rostov State Economic University (RINH), 69 Bolshaya Sadovaya St., Rostov-on-Don, 344002, Russia

e-mail: my.virus.kaspersky@gmail.com, mashechka-81@mail.ru, emine.halilaeva@yandex.ru

Abstract
In the modern world, the use of artificial intelligence (AI) is increasingly facing the risk of adversarial attacks on audio and images. This article explores this issue and presents the SGEC method as a means to minimize these risks. Various types of attacks on audio and images are discussed, including label manipulation, white-box and black-box attacks, leakage through trained models, and hardware-level attacks. The main focus is on the SGEC method, which offers data encryption and ensures their integrity in AI models. The article also examines other approaches to protect audio and images, such as dual verification and ensemble methods, access restriction and data anonymization, as well as the use of provably robust AI models.
Keywords: adversarial attacks; voiceprint protection; biometric data protection; steganography; data encryption; risks of adversarial attacks

For citation: Gerasimov V.M., Maslova M.A., Khalilayeva E.I. Protection against adversarial attacks on audio and images in artificial intelligence models using the SGEC method // Research result. Information technologies. – T.8, №2, 2023. – P. 53-60. DOI: 10.18413/2518-1092-2022-8-2-0-7

ВВЕДЕНИЕ

Развитие моделей искусственного интеллекта (ИИ), основанных на аудио и изображениях, открывает новые перспективы во множестве областей, включая медицину, автономные системы и мультимедийные приложения. Однако, с возросшим применением таких моделей, возникают и новые риски, связанные с состязательными атаками на аудио и изображения.

Состязательные атаки на аудио [1] и изображения [2] представляют собой специально разработанные методы введения искажений или шумов во входные данные моделей с целью обмана и искажения их результатов. Такие атаки могут быть использованы злоумышленниками для изменения выводов моделей ИИ и даже подрыва их безопасности.

В данной статье рассмотрим возможные риски состязательных атак на аудио и изображения в моделях искусственного интеллекта, обсудим способы манипуляции с данными, которые могут привести к неправильным результатам и искажениям, изучим последствия подобных атак и их потенциальные угрозы в различных сферах применения моделей на основе аудио и изображений.

В контексте защиты от этих рисков представлен метод SGEC [3], который предлагает шифрование данных, предназначенный для защиты системы ИИ от состязательных атак. Рассмотрим принципы работы и преимущества этого метода, а также его важность в обеспечении безопасности и надежности моделей ИИ на основе аудио и изображений.

Разбор возможных рисков состязательных атак на аудио и изображения и представление метода SGEC позволит нам получить более полное представление о безопасности и защите систем ИИ, а также определить наилучшие практики и меры предосторожности для предотвращения таких атак.

ОСНОВНАЯ ЧАСТЬ

Использование незащищённых данных в системах искусственного интеллекта (ИИ) сопряжено с рядом серьезных рисков. Вот некоторые из них:

1. Утечка конфиденциальной информации [4]. Если данные, содержащие личную или чувствительную информацию, попадут в руки злоумышленников, это может привести к утечке конфиденциальных данных. Например, в случае использования биометрических данных, таких как голос или лицо пользователей, утечка таких данных может привести к незаконному доступу к личным аккаунтам или идентификационным системам.

2. Нарушение приватности [5]. Незащищённые данные могут раскрывать личную информацию о пользователях, их привычках, предпочтениях и поведении. Это может нарушить их приватность и привести к нежелательной рекламе, мошенничеству или другим формам злоупотребления личной информацией.

3. Манипуляция и подделка данных [6]. Злоумышленники могут внести изменения в незащищённые данные, предоставленные системе ИИ, с целью искажения результатов или обмана системы. Например, подделка данных об обучающей выборке может привести к неправильным выводам или искаженным предсказаниям модели ИИ.

4. Атаки на систему ИИ [7]. Незащищённые данные могут использоваться для проведения атак на систему ИИ. Например, злоумышленники могут внедрить вредоносный код или манипулировать данными, чтобы нарушить работу или контроль над системой ИИ.

5. Утрата доверия пользователей [8]. Если данные пользователей не защищены должным образом, это может привести к потере доверия со стороны пользователей. Пользователи могут отказаться от использования системы ИИ или отказаться от предоставления своих данных из-за опасений по поводу их безопасности и конфиденциальности.

6. Юридические последствия [9]. Использование незащищённых данных может нарушать законодательство о защите данных, такое как общий регламент по защите данных

(GDPR) в Европейском союзе. Нарушение таких правил может привести к юридическим последствиям, включая штрафы и судебные разбирательства.

Учитывая эти риски, защита данных и обеспечение безопасности системы ИИ становятся критически важными аспектами, чтобы защитить пользователей, предотвратить утечки информации и обеспечить доверие к технологии ИИ [12].

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ И ИХ ОБСУЖДЕНИЕ

Применение рисков, связанных с состязательными атаками на аудио и изображения, позволяет системе нормально функционировать путем обеспечения ее безопасности и защиты от потенциальных угроз.

Путем изучения и понимания возможных рисков, связанных с состязательными атаками, система ИИ может принять соответствующие меры для защиты своих моделей и данных. Это позволяет обнаруживать и предотвращать попытки искажения или подмены аудио и изображений, которые могут повлиять на точность и достоверность результатов моделей ИИ.

Таблица

Риски состязательных атак и их описание

Table

Risks of adversarial attacks and their description

Риски информационной безопасности	**Описание**
1. Искажение разметки	Злоумышленники могут изменять метаданные и разметку данных, вводя искажения, чтобы ввести в заблуждение систему ИИ.
2. Искажение обучающей выборки	Злоумышленники могут изменять обучающую выборку данных, вводя искажения или злонамеренные примеры, для искажения работы системы ИИ.
3. Атаки "белого ящика" и "черного ящика"	Злоумышленники могут использовать атаки "белого ящика" и "черного ящика" для взлома системы ИИ путем доступа к ее внутренним параметрам или ввода вредоносных данных.
4. Дискретные правила обнаружения на основе ML	Злоумышленники могут использовать методы обхода и обмана системы ИИ, чтобы избежать обнаружения искусственным интеллектом, работающим на основе дискретных правил.
5. Атаки на предобученные и аутсорсинговые ML-модели	Злоумышленники могут нацелиться на предобученные модели и аутсорсинговые модели, пытаясь получить доступ к их конфиденциальным данным или вводя вредоносные данные.
6. Утечки через обученные модели	Злоумышленники могут использовать утечки информации через обученные модели, чтобы получить доступ к конфиденциальным данным, используемым в системе ИИ.
7. Атаки на уровне железа	Злоумышленники могут проводить физические атаки на инфраструктуру системы ИИ, включая атаки на железо и перехват электромагнитных излучений.

Таблица представляет основные риски информационной безопасности, связанные с защитой от состязательных атак на аудио и изображения в моделях искусственного интеллекта. Они могут нанести вред работе системы ИИ и утечке конфиденциальных данных. Применение метода SGEC позволяет снизить вероятность возникновения данных рисков и обеспечить безопасность системы ИИ.

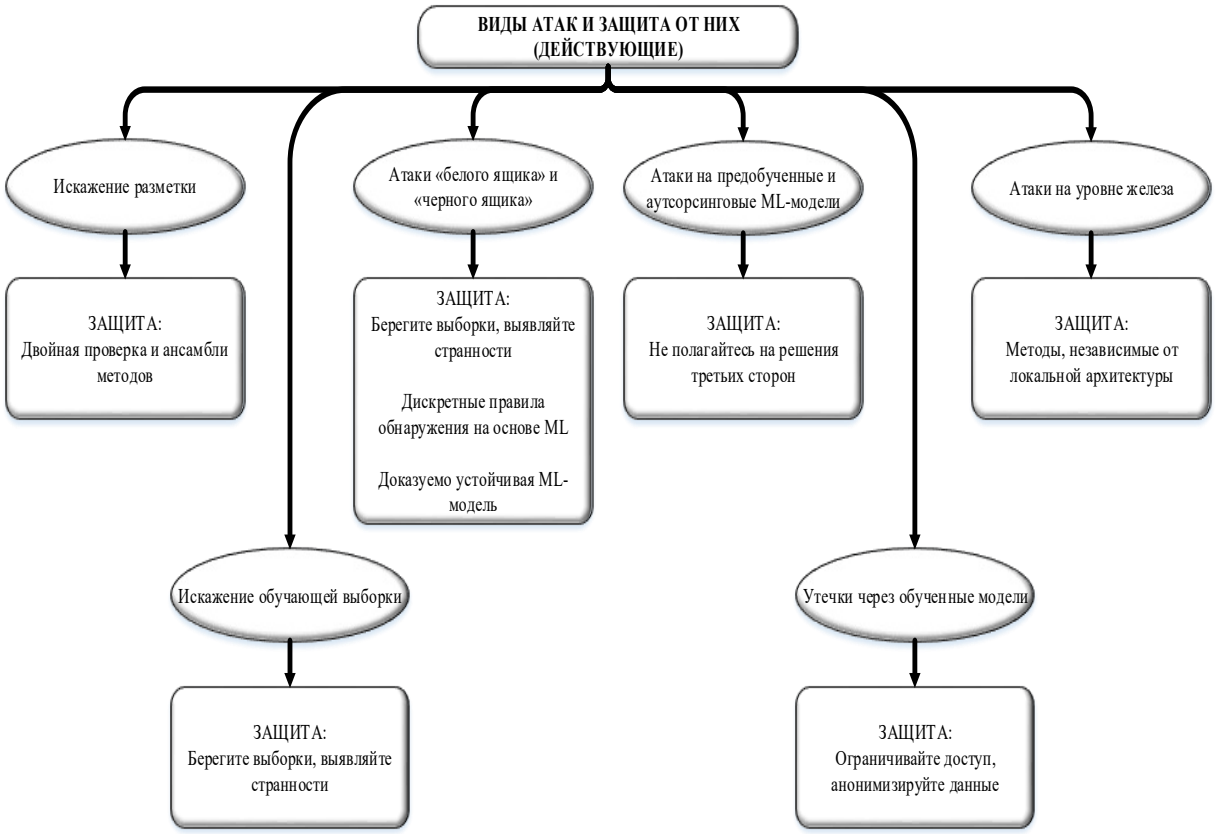

Рис. 1. Виды атак на систему ИИ и защита от них
Fig. 1. Types of attacks on AI systems and their defense

Использование метода SGEC, который предлагает шифрование данных [10], позволяет системе ИИ обеспечить безопасность и надежность при обработке аудио и изображений. Этот метод помогает предотвратить несанкционированный доступ к данным, а также защищает их от внешних вмешательств и состязательных атак.

Благодаря реализации этих мер защиты система ИИ может сохранять свою функциональность и надежность. Она может продолжать точно обрабатывать и анализировать аудио и изображения, основываясь на надежных данных и получая достоверные результаты. Это позволяет системе ИИ успешно выполнять свои задачи и быть полезной в различных сферах применения, включая медицину, автономные системы и мультимедийные приложения.

Таким образом, применение данных рисков и метода SGEC способствует нормальному функционированию системы ИИ, обеспечивая ее защиту от возможных атак, сохранение безопасности данных и достоверность результатов. Это важные аспекты для дальнейшего развития и успешного применения моделей ИИ на основе аудио и изображений.

Использование метода SGEC. Защита от состязательных атак на аудио и изображения является критически важным аспектом в области искусственного интеллекта (ИИ). Состязательные атаки – это попытки искажения, изменения или подмены данных в целях обмана системы ИИ и получения нежелательных результатов. Эти атаки могут иметь серьезные последствия, включая неверные диагнозы в медицинской области, ошибочные решения в автономных системах или фальсификацию мультимедийного контента.

Если акцентировать внимание на аудио и изображениях, то состязательные атаки могут применяться для изменения звуковых сигналов, таких как речь [11], или частичное (полное) искажение изображения. Например, злоумышленники создают аудио-сигналы, которые похожи на белый шум, позволяющий обмануть систему распознавания речи и дестабилизировать работу системы. Также атаки на изображения могут включать добавление или удаление определенных

элементов внутри определенного кадра. Подобные манипуляции над медиа-контентом может привести к ошибочным результатам анализа или распознавания объектов.

В итоге, подобные действия злоумышленников, которые используют состязательные атаки на системы ИИ не вызывает доверия и надёжность у пользователей — система может давать некорректные (неверные) результаты. Поэтому необходимо принимать меры для защиты моделей ИИ от таких атак.

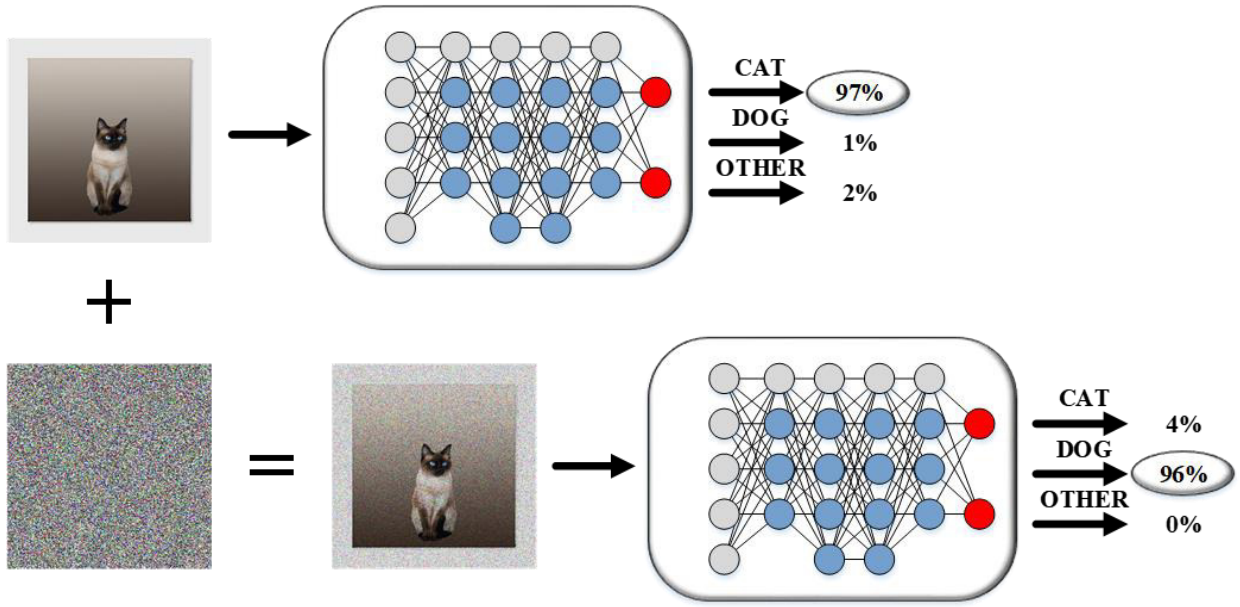

Рис. 2. Возможная атака на ИИ, путём зашумления данных

Fig. 2. Potential attack on AI through data perturbation

Метод SGEC представляет собой один из подходов, предлагающих решение для защиты данных аудио и изображений в системах ИИ. Этот метод основывается на шифровании данных путем генерации криптографических ключей и использования их для защиты и аутентификации данных. SGEC позволяет предотвратить несанкционированный доступ к данным и обеспечить их конфиденциальность и целостность.

Применение метода SGEC позволяет системе ИИ нормально функционировать, так как это обеспечивает ее защиту от возможных состязательных атак и гарантирует правильность и достоверность результатов. Защищенные данные позволяют системе ИИ принимать обоснованные решения на основе надежных и целостных аудио и изображений.

Однако следует отметить, что защита от состязательных атак – это непрерывный процесс, поскольку злоумышленники постоянно разрабатывают новые методы и алгоритмы для обмана систем ИИ. Поэтому необходимо постоянно совершенствовать методы защиты и проводить регулярные аудиты системы для выявления потенциальных уязвимостей и улучшения механизмов защиты.

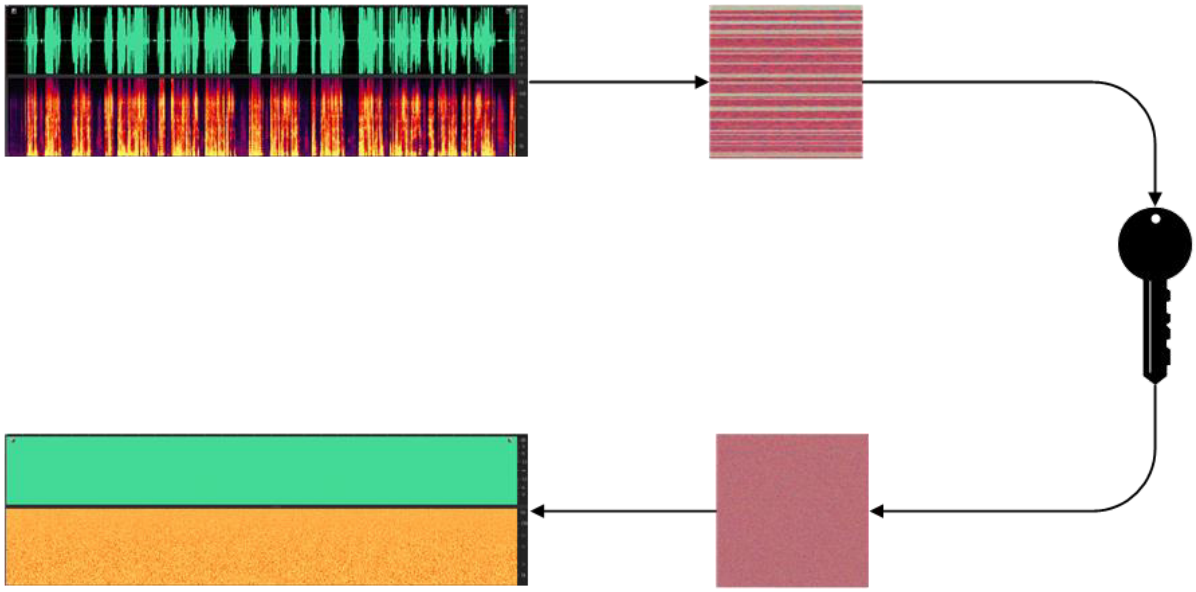

Рис. 3. Пример защиты голосовых данных

Fig. 3. Example of voice data protection

В целом, защита от состязательных атак на аудио и изображения в моделях ИИ является важной задачей для обеспечения надежности и безопасности систем ИИ. Применение метода SGEC и других подобных подходов способствует нормальному функционированию системы, обеспечивая ее защиту от атак, сохранение конфиденциальности и правильность обработки аудио и изображений.

ЗАКЛЮЧЕНИЕ

В заключении можно подчеркнуть важность защиты от состязательных атак на аудио и изображения в моделях искусственного интеллекта. Эти атаки могут серьезно подорвать надежность и безопасность систем ИИ, особенно тех, которые работают с конфиденциальными данными пользователей.

Применение метода SGEC, предложенного в данной статье, представляет эффективный подход к защите от таких атак. Шифрование данных и обеспечение их целостности помогают предотвратить изменение искажения данных, а также предотвращают несанкционированный доступ к информации.

Однако следует отметить, что разработка методов защиты информационной безопасности является непрерывным процессом. С появлением новых атак и методов обхода необходимо продолжать исследования и развивать новые подходы для обеспечения безопасности систем ИИ.

В целом, применение метода SGEC и других мер безопасности поможет снизить риски состязательных атак на аудио и изображения в моделях искусственного интеллекта. Это способствует созданию более надежных и безопасных систем ИИ, которые могут быть успешно применены в различных областях, сохраняя конфиденциальность и целостность данных.

Благодарность. Работа выполнена в рамках Соглашения от 30.06.2022 г. № 40469-21/2022-к.

Список литературы

1. Esmaeilpour M., Cardinal P., Koerich A. L. A robust approach for securing audio classification against adversarial attacks //IEEE transactions on information forensics and security. – 2019. – Т. 15. – С. 2147-2159.

2. Xu H. et al. Adversarial attacks and defenses in images, graphs and text: A review //International Journal of Automation and Computing. – 2020. – Т. 17. – С. 151-178.

3. Свидетельство о государственной регистрации программы для ЭВМ № 2022663168 Российская Федерация. SGEC-система "BIOM" для шифрования и сокрытия голосовых данных пользователей на сервере: № 2022662279: заявл. 27.06.2022: опубл. 12.07.2022 / В. М. Герасимов, М. А. Маслова; заявитель Федеральное государственное автономное образовательное учреждение высшего образования «Севастопольский государственный университет». – EDN FJQWGB.

4. Clark D., Hunt S., Malacaria P. Quantitative analysis of the leakage of confidential data // Electronic Notes in Theoretical Computer Science. – 2002. – Т. 59. – №. 3. – С. 238-251.

5. Martin K. The penalty for privacy violations: How privacy violations impact trust online // Journal of Business Research. – 2018. – Т. 82. – С. 103-116.

6. Yang J. et al. Msta-net: forgery detection by generating manipulation trace based on multi-scale self-texture attention //IEEE transactions on circuits and systems for video technology. – 2021. – Т. 32. – №. 7. – С. 4854-4866.

7. Li G. et al. DeSVig: Decentralized swift vigilance against adversarial attacks in industrial artificial intelligence systems //IEEE Transactions on Industrial Informatics. – 2019. – Т. 16. – №. 5. – С. 3267-3277.

8. Meeßen S. M. et al. Trust is essential: positive effects of information systems on users' memory require trust in the system //Ergonomics. – 2020. – Т. 63. – №. 7. – С. 909-926.

9. Lupton M. Some ethical and legal consequences of the application of artificial intelligence in the field of medicine //Trends Med. – 2018. – Т. 18. – №. 4. – С. 100147.

10. Герасимов, В. М. Комплексная система защиты биометрического голосового отпечатка от воздействия кибермошенников / В. М. Герасимов // XI Конгресс молодых учёных: Сборник научных трудов, Санкт-Петербург, 04–08 апреля 2022 года. – Санкт-Петербург: федеральное государственное автономное образовательное учреждение высшего образования "Национальный исследовательский университет ИТМО", 2022. – С. 72-76. – EDN VTVBBS.

11. Герасимов, В. М. Возможные угрозы и атаки на систему голосовой идентификации пользователя / В. М. Герасимов, М. А. Маслова // Научный результат. Информационные технологии. – 2022. – Т. 7, № 1. – С. 32-37. – DOI 10.18413/2518-1092-2022-7-1-0-4. – EDN JBCXMF.

12. Разработка программного модуля системы распознавания лиц с использованием метода Виолы – Джонса / М. И. Ожиганова, С. М. Арванова, А. А. Абитов, И. А. Уначев // Цифровая трансформация науки и образования: Сборник научных трудов II Международной научно-практической конференции, НАЛЬЧИК, 01–04 октября 2021 года. – НАЛЬЧИК, 2021. – С. 271-277. – EDN NRFFLF.

References

1. Esmaeilpour M., Cardinal P., Koerich A.L. A robust approach for securing audio classification against adversarial attacks //IEEE transactions on information forensics and security. – 2019. – T. 15. – P. 2147-2159.

2. Xu H. et al. Adversarial attacks and defenses in images, graphs and text: A review // International Journal of Automation and Computing. – 2020. – T. 17. – P. 151-178.

3. Certificate of state registration of the computer program No. 2022663168 Russian Federation. SGEC-system "BIOM" for encrypting and hiding the voice data of users on the server: No. 2022662279: App. 06/27/2022: publ. July 12, 2022 / V.M. Gerasimov, M.A. Maslova; applicant Federal State Autonomous Educational Institution of Higher Education "Sevastopol State University". – EDN FJQWGB.

4. Clark D., Hunt S., Malacaria P. Quantitative analysis of the leakage of confidential data // Electronic Notes in Theoretical Computer Science. – 2002. – T. 59. – №. 3. – P. 238-251.

5. Martin K. The penalty for privacy violations: How privacy violations impact trust online // Journal of Business Research. – 2018. – T. 82. – P. 103-116.

6. Yang J. et al. Msta-net: forgery detection by generating manipulation trace based on multi-scale self-texture attention // IEEE transactions on circuits and systems for video technology. – 2021. – T. 32. – №. 7. – P. 4854-4866.

7. Li G. et al. DeSVig: Decentralized swift vigilance against adversarial attacks in industrial artificial intelligence systems //IEEE Transactions on Industrial Informatics. – 2019. – T. 16. – №. 5. – P. 3267-3277.

8. Meeßen S. M. et al. Trust is essential: positive effects of information systems on users' memory require trust in the system //Ergonomics. – 2020. – T. 63. – №. 7. – P. 909-926.

9. Lupton M. Some ethical and legal consequences of the application of artificial intelligence in the field of medicine //Trends Med. – 2018. – T. 18. – №. 4. – P. 100147.

10. Gerasimov, V. M. Comprehensive system for protecting a biometric voice print from the effects of cyber fraudsters / V.M. Gerasimov // XI Congress of Young Scientists: Collection of scientific papers, St. Petersburg,

April 04–08, 2022. - St. Petersburg: Federal State Autonomous Educational Institution of Higher Education "National Research University ITMO", 2022. – P. 72-76. – EDN VTVBBS.

11. Gerasimov, V.M. Possible threats and attacks on the user's voice identification system / V.M. Gerasimov, M.A. Maslova // Scientific result. Information Technology. – 2022. – V. 7, No. 1. – P. 32-37. – DOI 10.18413/2518-1092-2022-7-1-0-4. – EDN JBCXMF.

12. Ozhiganova M. I., Arvanova S. M., Abitov A. A., Unachev I. A. Development of a software module for a face recognition system using the Viola-Jones method // Digital transformation of science and education: Collection of scientific papers II International Scientific and Practical Conference, NALCHIK, October 01–04, 2021. - NALCHIK, 2021. – P. 271-277. – EDN NRFFLF.

Герасимов Виктор Михайлович, инженер, студент первого курса магистратуры направления «Безопасность систем искусственного интеллекта» факультета Безопасности Информационных Технологий (БИТ)
Маслова Мария Александровна, старший преподаватель кафедры Информационная безопасность Института информационных технологий, аспирант, младший научный сотрудник Ростовского государственного экономического университета (РИНХ)
Халилаева Эмине Илимдаровна, студент первого курса магистратуры кафедры «Информационная безопасность» Института информационных технологий

Gerasimov Viktor Mikhailovich, engineer, a first-year master's student in the field of "Security of Artificial Intelligence Systems" faculty of the Security Information Technology (SIT)
Maslova Maria Alexandrovna, Senior Lecturer of the Department Information security Institute of Information Technologies, postgraduate student, junior researcher Rostov State Economic University (RINH)
Khalilayeva Emine Ilimdarovna, a first-year master's student in the field of the Department «Information security», Institute of Information Technology