

Повышение качества подготовки будущих специалистов по информационной безопасности в практике разработки чат-ботов

Improving the quality of training for future information security specialists in the practice of chatbot development

Авторы статьи

Шилова Зоя Вениаминовна,
кандидат педагогических наук, доцент кафедры высшей математики Института кибербезопасности и цифровых технологий ФГБОУ ВО «МИРЭА – Российский технологический университет», доцент кафедры ФН-12 ФГАОУ ВО «Московский государственный технический университет имени Н. Э. Баумана (национальный исследовательский университет)», г. Москва, Российская Федерация
zoia@soi.su
ORCID ID: 0000-0003-1715-2513

Елизарова Наталья Анатольевна,
кандидат педагогических наук, доцент кафедры высшей математики Института кибербезопасности и цифровых технологий ФГБОУ ВО «МИРЭА – Российский технологический университет», г. Москва, Российская Федерация
elizarova77@mail.ru
ORCID ID: 0009-0006-3117-4398

Ивахненко Наталья Николаевна,
кандидат физико-математических наук, доцент кафедры физики ФГБОУ ВО «Российский государственный аграрный университет – МСХА имени К. А. Тимирязева»; доцент кафедры ФН-12 ФГАОУ ВО «Московский государственный технический университет имени Н. Э. Баумана (национальный исследовательский университет)», г. Москва, Российская Федерация
yulduz1977@mail.ru
ORCID ID: 0000-0002-7328-7633

Конфликт интересов

Конфликт интересов не указан

Authors of the article

Zoya V. Shilova,
Candidate of Pedagogical Sciences, Associate Professor, Department of Higher Mathematics, Institute of Cybersecurity and Digital Technologies, "MIREA – Russian Technological University"; Associate Professor, Department FN-12, Bauman Moscow State Technical University (National Research University), Moscow, Russian Federation
zoia@soi.su
ORCID ID: 0000-0003-1715-2513

Natalya A. Elizarova,
Candidate of Pedagogical Sciences, Associate Professor, Department of Higher Mathematics, Institute of Cybersecurity and Digital Technologies, "MIREA – Russian Technological University", Moscow, Russian Federation
elizarova77@mail.ru
ORCID ID: 0009-0006-3117-4398

Natalya N. Ivakhnenko,
Candidate of Physical and Mathematical Sciences, Associate Professor, Department of Physics, Russian State Agrarian University – Moscow Timiryazev Agricultural Academy; Associate Professor, Department FN-12, Bauman Moscow State Technical University (National Research University); Moscow, Russian Federation
yulduz1977@mail.ru
ORCID ID: 0000-0002-7328-7633

Conflict of interest statement

Conflict of interest is not declared

Поступила в редакцию <i>Received</i>	24.06.26	Получена положительная рецензия <i>Received a positive review</i>	30.07.26
Принята к публикации <i>Accepted for publication</i>	30.07.26	Опубликована <i>Published</i>	30.09.26



Для цитирования

Шилова З. В., Елизарова Н. А., Ивахненко Н. И. Повышение качества подготовки будущих специалистов по информационной безопасности в практике разработки чат-ботов // Научно-методический электронный журнал «Концепт». – 2026. – № 09. – С. 337–351. – URL: <https://e-koncept.ru/2026/261250.htm> – DOI: 10.24412/2304-120X-2026-11250

For citation

Z. V. Shilova, N. A. Elizarova, N. N. Ivakhnenko, Improving the quality of training for future information security specialists in the practice of chatbot development // Scientific-methodological electronic journal "Koncept". – 2026. – No. 09. – P. 337–351. – URL: <https://e-koncept.ru/2026/261250.htm> – DOI: 10.24412/2304-120X-2026-11250

Аннотация

Модернизация высшего образования открывает перспективы использования искусственного интеллекта (далее – ИИ) при обучении специалистов в области информационной безопасности. Учебная деятельность, поддержанная чат-ботами на основе ИИ, обладает определенным потенциалом для повышения качества подготовки студентов. Цель исследования – выявить особенности взаимодействия будущих специалистов по информационной безопасности в практике разработки чат-ботов, влияющие на повышение качества их подготовки. Ведущий метод – информационное моделирование в виртуальной среде конструктора чат-ботов. На этапе оценки качества подготовки студентов применяются материалы контрольной работы из 60 вопросов. База эксперимента: МИРЭА – Российский технологический университет, Институт кибербезопасности и цифровых технологий. Задействовано 84 студента, обучающихся по направлению подготовки 10.03.01 «Информационная безопасность автоматизированных систем». Основные результаты исследования включают описание деятельности студентов по проектированию и созданию чат-ботов. Полученные заключения и выводы – основа для совершенствования программы подготовки специалистов IT-отрасли. В результатах представлены идеи методического подхода, направленного на усиление влияния следующих факторов для повышения качества подготовки студентов: постепенная, обусловленная практической необходимостью интеграция элементов ИИ; соблюдение правил кибербезопасности и норм этики. Теоретическая значимость: выявленные возможности чат-ботов уточняются применительно к обучению студентов, способных разрабатывать инновационные решения в сфере кибербезопасности и цифровых технологий. Практическая значимость: определены факторы, влияющие на эффективность включения чат-ботов, функционирующих на базе ИИ, на уровень подготовки высококвалифицированных кадров из IT-сферы. Научная новизна: обосновывается потенциал включения практики по конструированию чат-ботов в обучение специалистов по информационной безопасности. В заключении сформулированы особенности работы студентов при проектировании и создании чат-ботов: поддержка условий для понимания важности профессии; сочетание фундаментальной теории и практики виртуального взаимодействия; информирование обучающихся об ограничениях использования ИИ; учет проблем кибербезопасности.

Abstract

The modernization of higher education opens up prospects for the use of artificial intelligence (AI) in the training of information security specialists. Educational activities supported by AI-based chatbots have a certain potential to improve the quality of student training. The purpose of the study is to identify the interaction features of future information security specialists in the practice of developing chatbots that affect the improvement of their training quality. The leading method is information modeling in the virtual environment of a chatbot constructor. At the stage of assessing the quality of students' training, the materials of the 60-question test paper are used. Experimental base: MIREA – Russian Technological University, Institute of Cybersecurity and Digital Technologies. 84 students studying in the area of training 10.03.01 "Information security of automated systems" are involved. The main research results include a description of students' activities in designing and creating chatbots. The conclusions obtained are the basis for improving the training program for IT industry specialists. The results present the ideas of a methodological approach aimed at strengthening the influence of the following factors to improve the quality of student training: gradual integration of AI elements due to practical necessity; compliance with cybersecurity rules and ethical standards. Theoretical significance – the identified chatbot capabilities are being clarified in relation to the training of students who are able to develop innovative solutions in the field of cybersecurity and digital technologies. Practical significance – the factors influencing the effectiveness of the inclusion of AI-based chatbots in the level of training of highly qualified personnel from the IT sector have been identified. Scientific novelty: the potential of including the practice of designing chatbots in the training of information security specialists is substantiated. In conclusion, the specific aspects of students' work in designing and creating chatbots are outlined: fostering an understanding of the profession's importance; combining fundamental theory with the practice of virtual interaction; informing students about the limitations of AI usage; and addressing cybersecurity issues.

Ключевые слова

цифровые инновации, информационные технологии, искусственный интеллект, защита данных, конструктор чат-ботов, кибербезопасность

Key words

digital innovations, information technology, artificial intelligence, data protection, chatbot constructor, cybersecurity

Благодарности

Авторы выражают благодарность ФГБОУ ВО «МИРЭА – Российский технологический университет» за поддержку цифровых инноваций и применение технологий ИИ в подготовке высококвалифицированных кадров по информационной безопасности.

Acknowledgements

The authors express their gratitude to MIREA – Russian Technological University for supporting digital innovations and applying AI technologies in the training of highly qualified personnel in the field of information security.

Введение / Introduction

Эксперты в области IT и информационной безопасности на Саммите по цифровым инновациям (проходившем в Бухаресте в 2025 году) определили тенденции и тренды развития цифрового будущего для ведущих стран мира. Лидеры IT-индустрии особенно выделили растущую роль ИИ в сфере кибербезопасности и цифровой трансформации [1]. На Саммите были продемонстрированы достижения в области цифровой идентификации, защиты данных, автоматизированных устройств и устойчивых технологий. Большинство ученых поддержало идею о том, что необходимо вносить корректировки в программы подготовки специалистов IT-сферы с учетом новых вызовов и киберугроз.

В Указе Президента РФ «О развитии искусственного интеллекта в Российской Федерации» определены стратегические положения и векторы развития, которых образовательным учреждениям следует придерживаться при выполнении научных исследований и разработок на базе ИИ. В частности, регламентирована необходимость повышения уровня подготовки и компетенций специалистов в отрасли IT и информационной безопасности [2]. В качестве реализации указанных направлений развития отметим проект, который представили ученые Института образования НИУ ВШЭ. Проект выполнен в коллаборации со студентами, получающими специальность в IT-сфере [3]. Разработчики сконструировали и продемонстрировали на практике чат-бот, позволяющий автоматизировать процесс саморегулируемого обучения и управлять вовлеченностью обучающихся. Представленная разработка реализована в рамках программы «Приоритет-2030». Следовательно, потенциально подобная деятельность может усилить программы подготовки студентов и других вузов, других городов и стран.

В исследовании Т. А. Тронь выполнен анализ современного состояния и трудностей подготовки специалистов по информационной безопасности [4]. В качестве одной из ключевых проблем автор отмечает существенный разрыв между уровнем практической подготовки выпускников и вызовами IT-сферы. Например, многие специалисты знают угрозы «утечки» данных, механизмы нарушения конфиденциальности информации, требования к надежностям паролей. Однако применение полученных знаний на практике сталкивается с проблемой постоянного обновления спектра угроз и хищений. К непрерывному обучению, стрессу и деятельности в условиях неопределенности значительная часть выпускников вузов оказывается неподготовленной.

Д. Хэншоу, К. Салливан указывают, что интеграция ИИ в сферу высшего образования предоставляет широкий спектр возможностей в плане повышения мотивации и вовлеченности обучающихся [5].

Э. Тоени, Л. Фрайер изучают влияние взаимодействия студентов с чат-ботом на ключевые факторы, способствующие успешному обучению (интерес, вовлеченность) [6]. Учеными в ходе проведенного эксперимента не удалось подтвердить значительный положительный эффект ресурсов ИИ в отношении повышения успеваемости будущих специалистов. Как следствие, авторы обосновывают необходимость проведения дополнительных исследований в целях подтверждения дидактического потенциала чат-ботов и применения их в высшем образовании.

Таким образом, с одной стороны, интеграция чат-ботов на основе ИИ в обучение специалистов по информационной безопасности – важное условие для повышения качества их подготовки. С другой стороны, существует разрыв между реальным уровнем подготовки выпускников и вызовами IT-отрасли.

Гипотеза исследования: организация работы будущих IT-специалистов по проектированию и созданию чат-ботов позволит обеспечить дополнительные условия для повышения качества подготовки студентов.

Цель работы – выявить особенности взаимодействия будущих специалистов по информационной безопасности в практике разработки чат-ботов, влияющие на повышение качества их подготовки.

Задачи исследования:

- уточнить трудности и перспективы включения чат-ботов в обучение специалистов по кибербезопасности и автоматизации работы систем;
- описать идеи методического подхода, предполагающего активное использование конструкторов чат-ботов в обучении специалистов по защите информации;
- экспериментально проверить эффективность идей предлагаемого подхода.

Обзор литературы / Literature review

Ч. Эзеквем, Ч. Учеджи, Д.Ч. Экенеме устанавливают, что активное внедрение ИИ в сферу кибербезопасности изменило стратегии национальной безопасности для многих стран мира [7]. Авторами готовность к использованию ИИ в государственных планах по кибербезопасности рассматривается на примере трех различных моделей управления: США, Китая и Европейского союза. Выполненный учеными анализ показал, что интеллектуальная зрелость отраслей экономики и человеческий капитал страны являются основополагающими факторами, определяющими готовность нации к инновациям времени.

А. Архипова рассматривает вопросы повышения качества подготовки специалистов по информатизации и защиты автоматизированных систем [8]. Автор отмечает, что в программы обучения высококвалифицированных ИТ-специалистов следует обязательно добавлять модули, включающие изучение основ обеспечения безопасности сетей, систем ИИ и работу с виртуальными ассистентами.

М. Резниченко, Е. Помельникова указывают, что подготовка специалистов по информационной безопасности в системе высшего образования считается одной из первоочередных стратегических задач Российской Федерации в условиях международной нестабильности [9]. Авторами на практических примерах доказано, что у студентов, обучающихся на соответствующих специальностях, необходимо формировать готовность к постоянному самообучению, критическое мышление и креативность, стрессоустойчивость. Для развития этих востребованных навыков ученые предлагают использовать проблемно-поисковые методы, инновационные цифровые технологии и виртуальные среды обучения.

С. Свапна, В. Сивалингам определяют, что внедрение ИИ в сферу кибербезопасности произвело настоящую революцию в этой области [10]. Инновационные инструменты позволяют на качественно другом уровне выявлять киберугрозы, оперативно на них реагировать и устранять последствия кибератак с максимальным эффектом. Авторы представляют эволюцию механизмов защиты в сфере кибербезопасности от традиционных подходов к системам с использованием ИИ. Исследователи выявляют проблемы этики и конфликта интересов, обусловленные внедрением нейросетей.

Е. В. Щедрина, Е. В. Соболева, О. Н. Ивашова описывают опыт применения ИИ в подготовке цифровых инженеров будущего [11]. Авторы представляют педагогические инновации, реализуемые на платформах аграрного вуза. Получение навыков коммуникации в виртуальной среде (в том числе с «неизвестными» собеседниками в чате), по заключениям ученых, важная часть подготовки кадров, максимально востребованных на рынке труда.

Ф. Супангкат, О. Рамадани, Р. Путранто, И. Альбана указывают, что достижения в области технологий ИИ привели к значительным изменениям в области безопасности данных [12]. Новые цифровые технологии предоставляют IT-специалистам инструменты, позволяющие не только быстрее и точнее обнаруживать киберугрозы, но и оперативно реагировать на них. В исследовании проанализирована роль ИИ в повышении безопасности данных с помощью различных методов (машинного обучения, чат-ботов и др.). Ученые показывают, что ИИ эффективен в различных аспектах безопасности, таких как анализ поведения пользователей и управление идентификацией. Однако, по мнению авторов, реализация преимуществ ИИ на практике требует разработки специального стратегического подхода, подразумевающего создание более прозрачных и безопасных автоматизированных систем. Последнее, в свою очередь, невозможно без сотрудничества между различными заинтересованными сторонами (школы, университеты, промышленные компании). Представленный анализ подчеркивает ключевую роль автоматизированных систем, функционирующих на базе ИИ, в преобразовании сферы кибербезопасности. Также авторы указывают на необходимость тщательного контроля всех этапов разработки новых цифровых продуктов (в частности, виртуальных помощников).

А. Ифелебуэгу, М. Кулуме, П. Херукут отмечают, что ИИ продолжает активно внедряться во все сферы жизни [13]. И образование в этом плане не является исключением. Авторы указывают, что некоторые приложения на основе ИИ в образовании, например чат-боты, открывают перед педагогами интересные возможности. Однако включение ИИ в обучение задает преподавателям и непростые задачи: например, как остановить распространение дезинформации, как выявить и предотвратить плагиат.

М. Амин, Х. Расид, А. Акмаль указывают, что развитие ИИ в сфере образования открывает широкие возможности для разработки учебных материалов нового качества [14], в частности, разработки ресурсов, включающих инструменты, имитирующие общение с наставником. Ученые рассматривают внедрение сложных генеративных систем для общения в образовательные чат-боты [15]. Подобные инструменты, по выводам авторов, призваны улучшить процесс обучения и взаимодействие учащихся. Исследователи пытаются выяснить, каких результатов можно достичь с помощью таких передовых систем; подходят ли они для преподавания в вузах; какие существуют проблемы их внедрения. В своих рекомендациях авторы настаивают на том, что ключевыми элементами подобных инноваций являются этика в сфере ИИ, методы персонализированного обучения, а также комбинация индивидуальной и групповой работы.

В. Вибулиасарин, К. Вибулиасарин, Ф. Тиранант, Н. Джиноват, П. Буньякитанонт изучают эффективность чат-ботов, управляемых искусственным интеллектом, и выявляют их педагогические возможности [16]. Они выполняют обзор на основе 30 эмпирических исследований, опубликованных в период с 2020 по 2024 год. Ученые выделяют дидактический потенциал инструментов, отвечающих за поддержку таких функций, как обратная связь в режиме реального времени, новые возможности для практики. Авторы считают, что оптимальное использование чат-ботов зависит от вдумчивого подхода пользователей, от запрограммированных в алгоритмах инструкций разработчика (человека).

М. Пикхарт, Л. Аль-Обайди представляют спектр потенциальных рисков, связанных с использованием ИИ в сфере высшего образования [17]. Авторы выражают мнения группы преподавателей университетов из Чехии и Ирака. Они настаивают на необходимости проведения дальнейших исследований, в которых будет учитываться (оцениваться) роль и влияние разного рода виртуальных помощников и цифровых агентов.

К. Гилберт, М. Гилберт отмечают, что благодаря стремительному развитию технологий появление дипфейков и цифровой дезинформации является одновременно

и мощным инструментом, и серьезной проблемой [18]. Авторы подчеркивают роль ИИ как в качестве движущей силы инноваций, так и в качестве защитного механизма. Они выявляют разные этические и политические аспекты, а также необходимость повышения прозрачности, подотчетности и медиаграмотности. Ученые настаивают на координации деятельности бизнес-структур, государственных учреждений и образовательных организаций.

Х. Симос, Е. Цагкурни, Н. Бардис, Н. Дукас выявляют, что стремительное развитие цифровых технологий кардинально изменило систему образования [19]. Наиболее значительные изменения, по выводам авторов, произошли в дисциплинах STEM. Они заключают, что среди всех цифровых технологий образовательные чат-боты являются наиболее интерактивными системами. Например, с их помощью обучающиеся могут постоянно взаимодействовать с системами поддержки обучения, оперативно получать обратную связь с учетом своих индивидуальных потребностей. В выводах ученые определяют, что образовательные чат-боты – это мощный инструмент для цифровой трансформации естественно-научного, технологического, инженерного и математического образования.

Д. Джамалудин, М. Лиза, Г. Рахман, Э. Киссия, Г. Ваттимена, Дж. Батлолона развивают их идеи и обосновывают необходимость подготовки самих педагогов к применению элементов ИИ, образовательных чат-ботов для обучения будущих инженеров, математиков [20].

Е. В. Соболева, Т. Н. Суворова, Л. А. Шунина, П. М. Горев рассматривают проблемы и перспективы применения чат-ботов для развития эмоционального интеллекта выпускников педагогического вуза [21]. Авторы предлагают варианты организации практической деятельности студентов, в ходе которой происходит конструирование диалогового ассистента. Далее разработанный чат-бот студенты применяют на практике в школе.

С. Плойбут выполняет анализ литературы по вопросам применения чат-ботов с ИИ в образовании [22]. Для анализа были отобраны 30 статей, проиндексированных в Scopus и опубликованных в период с 2020 по 2025 год. Исследование показало, что чат-боты с ИИ в основном используются для персонализации обучения, повышения вовлеченности учащихся, развития навыков самоконтроля и оптимизации процесса решения задач управления. Автор выделяет и проблемные вопросы применения ИИ: обеспечение конфиденциальности данных, академическая честность, развитие навыков критического мышления.

В. Шарма, Др. Сехрават, М. Верма, Р. Шарма, А. Кумар высказывают обоснованные опасения по поводу применения чат-ботов с ИИ в высшем образовании [23]. Авторы выделяют дидактический потенциал образовательных чат-ботов: быстрые ответы на простые вопросы (с пояснениями), предоставление дополнительных материалов, поддержка в обучении. Чат-боты также могут выступать в роли ассистентов преподавателя, например, помогают восполнить пробелы в знаниях, возникающие из-за различных факторов.

В. И. Рой и К. А. Джанардханан отмечают, что вовлеченность студентов в процесс обучения инженерному делу – сложный методический процесс [24]. Р. Кумар, К. Аджит описывают роли чат-ботов в поддержке обучения студентов, например предоставление непрерывной персонализированной обратной связи [25].

Ф. Вибово, Х. Хасби, Т. Азиз, Д. Дарман, А. К. Карлин, Б. М. Ихсан формулируют вывод, заключающийся в том, что ИИ помогает обучающимся самостоятельно открывать для себя новые понятия [26]. Авторы указывают, что существует ограниченное количество эмпирических исследований, посвященных интеграции ИИ в обучение физике. Цель исследования Ф. Вибово, Х. Хасби, Т. Азиз, Д. Дарман, А. К. Карлин, Б. М. Ихсан заключается в разработке чат-бота с ИИ для изучения темы изменения климата.

К. Анвита, Т. Дурджай, К. Сатвика, Г. Гнанендра, А. Сельвараджан, С. Натараджан рассматривают вариант организации практической деятельности студентов по использованию ресурсов EduBot [27].

Д. Хэншоу, К. Салливан описывают опыт внедрения сервиса Spark [28]. Это помощник на основе ИИ, внедренный в Тихоокеанском университете Лос-Анджелеса. Исследование подчеркивает важность выбора коммуникативной стратегии, обоснованность интеграции инструментов ИИ в учебный процесс, необходимость высокого уровня цифровой грамотности и мастерства преподавателей.

А. С. Варламов анализирует голосовые ассистенты для поддержки клиентов по телефону и текстовые чат-боты [29]. А. Ф. Смык, Е. А. Гусева изучают вопросы влияния ИИ на инженерное образование в фокусе преподавания дисциплины «Физика» [30]. Предпринята попытка продемонстрировать возможности ИИ для решения проблем в ходе освоения курса физики в инженерном вузе.

А. А. Быков, О. М. Киселева выполняют классификацию виртуальных ассистентов по алгоритму взаимодействия, внешнему виду и функционалу [31]. Авторы описывают содержание (структуру диалогов) цифрового помощника для обучения физике.

О. В. Бойправ, Я. А. Клиндухов, С. Д. Мажаева указывают на важность решения проблемы роста угроз информационной безопасности в условиях стремительной цифровизации всех сфер жизни [32]. Н. Худер, П. И. Сигети, И. Б. Государев, М. Альжниди считают, что подготовка специалистов в области информационной безопасности должна включать изучение и практическое применение веб-ботов [33]. Веб-боты, в понимании авторов, это инструменты, которые используются поисковыми системами для индексации веб-страниц и сбора информации.

Выполненный анализ литературы позволяет объективно заключить:

– применение ИИ и чат-ботов в преподавании – актуальное направление в развитии высшего образования, в частности, для обучения специалистов по информационной безопасности;

интеграция ИИ и чат-ботов в подготовку специалистов ИТ-сферы сопровождается рядом организационных трудностей, необходимостью решения проблем этики и конфиденциальности.

Материалы и методы / Materials and methods

Работа будущих специалистов по информационной безопасности (информационное моделирование, проектирование и создание чат-ботов, конструирование диалогов с виртуальными собеседниками) организована на занятиях по дисциплине «Информатика». База опытно-экспериментальной работы (далее – ОЭР): Федеральное государственное бюджетное образовательное учреждение высшего образования «МИРЭА – Российский технологический университет», Институт кибербезопасности и цифровых технологий. Сокращенное наименование – РТУ МИРЭА (ИКБ).

Задействовано 84 студента, обучающихся по направлению подготовки 10.03.01 «Информационная безопасность автоматизированных систем». Средний возраст – 19 лет (20% – девушки, 80% – молодые люди). Все участники – студенты первого-второго курсов. Для разработки чат-ботов используется конструктор Senler (<https://help.senler.ru/>).

В основе диагностики уровня подготовки специалистов – тест, составленный из вопросов и заданий фонда оценочных средств по информатике. Всего 60 заданий: за правильный ответ на вопрос открытого типа – 2 балла, на вопрос закрытого типа –

1 балл. Определены уровни подготовки: «Наблюдатель» (от 0 до 29 баллов), «Испытатель» (от 30 до 79 баллов), «Конструктор» (от 80 до 90 баллов).

При статистической обработке данных использован критерий χ^2 Пирсона (онлайн-калькулятор – <https://medstatistic.ru/calculators/calchit.html>). Ограничения и условия критерия выполняются: объем выборки больше 30 респондентов, пересечения в них отсутствуют, сумма респондентов по каждой группе совпадает с общим числом студентов по направлению подготовки.

Результаты исследования / Research results

Организация работы студентов в информационной среде при конструировании чат-ботов

Работе будущих специалистов в области обеспечения информационной безопасности по конструированию чат-ботов предшествовало изучение ряда теоретических и практических модулей, например теоретические основы информатики (свойства информации и информационные процессы), проблемы цифровизации общества, современные цифровые технологии, нормативно-правовые документы в сфере ИТ. Обучающиеся получили опыт работы с сервисами Яндекс, интерактивными цифровыми ресурсами, HTML-страницами, QR-кодами. Студенты успешно справились с заданиями по установке защиты на текстовые документы, электронные таблицы, папки.

В рамках одного из лекционных занятий будущие специалисты по информационной безопасности изучили следующие базовые понятия: ИИ; чат-бот, функционирующий на базе ИИ. Студенты рассмотрели различные сервисы для конструирования чат-ботов: PuzzleBot, BotMan, Senler, Salebot и др.

Выяснено, что конструктор чат-ботов активно применяется в сфере ИТ. Создание и настройка чат-ботов с помощью конструктора – это быстрое и эффективное решение для компании, занимающейся продажей услуг или товаров. Созданный цифровой агент сможет самостоятельно общаться с клиентами, привлекать новую целевую аудиторию.

Многие из рассмотренных сервисов по конструированию чат-ботов обладают широким спектром возможностей, хорошим уровнем технической поддержки. Однако их интеграция зачастую предполагает использование Telegram. Работа последнего замедлена (заблокирована) на территории России. В этих условиях выбор Senler (<https://senler.ru>) является объективным и обоснованным.

Опишем далее логику работы студентов с конструктором по созданию чат-ботов.

I этап. Изучение возможностей, интерфейса и базовых инструментов. Сервис Senler – мощный и удобный конструктор чат-ботов, который интегрируется с социальной сетью «ВКонтакте». С помощью сервиса Senler можно автоматизировать общение с подписчиками, проводить тесты, викторины, квесты, собирать заявки и продавать товары.

Работа с инструментами Senler начинается с регистрации. Переходя по ссылке на сайт (<https://senler.ru>), пользователь получает доступ к главной странице ресурса.

Конструирование начинается с интеграции с социальной сетью «ВКонтакте». Отметим, что можно создать страницу или воспользоваться уже имеющейся у пользователя.

Далее появится окно для подтверждения входа через страницу социальной сети. При необходимости потребуется подтвердить свою электронную почту. Затем пользователь попадает в личный кабинет конструктора.

1.1. Нажмите на «+ Добавить канал» в правом верхнем углу экрана. Из предложенных возможностей выделите – «ВКонтакте». Здесь нужно из имеющихся групп

выбрать ту, к которой сообщество Senler будет иметь доступ. Это необходимо для того, чтобы разрабатывать опросы, квесты, викторины и т. д.

1.2. Проверьте, что канал появился. После успешного подключения в списке каналов появится Ваше сообщество. Например, данным сообществом может быть группа Института кибербезопасности и цифровых технологий.

Методическая особенность. Следует заранее оговориться, что для того, чтобы чат-боты сервиса Senler вообще работали, нужно перейти в целевое сообщество. В блоке «Управление» выбрать пункт «Сообщения» и найти «Возможности ботов». Здесь следует поставить галочку – «включить».

1.3. Обратите внимание на панель управления в целом и рассмотрите основные ее вкладки:

- рассылка – создание и отправка массовых сообщений подписчикам (по группам или всей базе);
- группы подписчиков – сегментация аудитории. Сюда попадают пользователи, которые подписались на рассылку. Можно создавать разные группы;
- подписчики – список всех пользователей, которые взаимодействовали с вашим ботом или подписались на рассылку;
- чат-боты – здесь создаются и редактируются сценарии ботов. Вы сейчас находитесь в разделе создания нового бота;
- аналитика – статистика по боту: сколько пользователей зашло, сколько завершило сценарий, на каких шагах ошибки;
- метки – инструмент для ручной маркировки подписчиков, например ВИП;
- триггеры – автоматические реакции на действия пользователя. Например, если написал слово «привет», запустить бота;
- заказы – если подключен магазин/товары ВК – здесь будут заказы от пользователей;
- процессы – фоновые задачи (импорт подписчиков, массовая рассылка, добавление в группы). Показывают прогресс выполнения.

1.4. К основному функционалу относится возможность «Отправка сообщений». В рамках диалогов с пользователем Вы можете выполнять следующие действия: отправлять текст; прикреплять вложения (изображения, документы и др.). После отправки Ваше сообщение сразу появляется в диалоге.

Когда пользователь отправляет сообщение: оно сразу появляется в открытом окне диалога; диалог поднимается вверх списка. Новые сообщения отмечаются как непрочитанные, но при открытии диалога они автоматически считаются прочитанными.

1.4.1. Фильтрация диалогов. Набор фильтров позволяет быстро находить нужные чаты и работает в несколько этапов.

1.4.2. Выбор подписчика. После выбора канала можно выбрать конкретных пользователей: найти подписчика по имени; выбрать одного или нескольких подписчиков.

II этап. Создание первого чат-бота. Методическая особенность. Перед созданием чат-ботов следует ознакомиться с «Правилами для ботов социальной сети “ВКонтакте”».

2.1. Переход в раздел чат-ботов. В левом меню кабинета выберите пункт «Чат-боты». Откроется страница со списком всех созданных (сконструированных) чат-ботов.

2.2. Создание нового бота. Нажмите кнопку «Новый бот» в правом верхнем углу страницы. Откроется форма для создания чат-бота.

2.3. Заполнение данных бота. В форме создания чат-бота заполните поля:

- название. Введите название чат-бота. Это имя будет отображаться в списке ботов и в конструкторе;
- ключ. Это уникальный идентификатор чат-бота в рамках канала. Нужен для идентификации, полезен, если названия ботов одинаковые. Заполняется автоматически на основе названия чат-бота. Ключ может содержать только цифры и латинские буквы. При необходимости ключ можно изменить вручную;
- теги (необязательно). Вы можете указать теги для удобной организации чат-ботов: начните вводить название тега; выберите существующий тег из списка или создайте новый.

2.4. Сохранение чат-бота. Нажмите кнопку «Сохранить».

III этап. Создание бота по направлению подготовки

Далее студенты выбирали среди доступных (открытых) сообществ «ВКонтакте» то, с которым бы планировали устроить виртуальный диалог в области информационной безопасности, например официальная страница университета (Института), Центр программирования и кибербезопасности, Школа кибербезопасности, Кибершкола МГУ и др.

Параллельно обучающиеся выбирали тематику для конструирования чат-бота. Например, «Все о киберугрозах», «Социальная инженерия», «Утечка данных», «Тренды и проблемы ИБ», «Импортозамещение», «Кибердом», «Доступ разрешен» и др.

Сконструированные чат-боты, описание логики информационного взаимодействия с пользователями канала студенты представляли в виде доклада и презентации на зачете по дисциплине.

Описание опытно-экспериментальной работы

На первом этапе ОЭР изучены и проанализированы сервисы для конструирования чат-ботов. Сформулированы 60 вопросов для тестирования. Приведем примеры вопросов.

Вопросы открытого типа: сколько бит нужно для представления восьмеричной цифры; перечислить средства охранной сигнализации; что называют параметрическим каналом утечки?

Пример вопроса закрытого типа: комплекс превентивных мер по защите конфиденциальных данных и информационных процессов на предприятии – это _____. Варианты ответов: «комплексное обеспечение ИБ»; «безопасность автоматизированной системы (далее – АС)»; «угроза ИБ»; «атака на АС».

Сформированы контрольная и экспериментальная группы. Далее определены уровни подготовки: «Наблюдатель» (от 0 до 29 баллов), «Испытатель» (от 30 до 79 баллов), «Конструктор» (от 80 до 90 баллов).

Наблюдатель (от 0 до 29 баллов) – студент зачастую не задумывается об этических проблемах, трудностях защиты данных при использовании современных цифровых устройств, технологий и сервисов ИИ. Он конструирует и интегрирует чат-боты только при существенной помощи преподавателя.

Испытатель (от 30 до 79 баллов) – студент знает многие актуальные (потенциальные) риски, проблемы и тенденции в сфере IT. Он не использует для выполнения заданий в виртуальной среде и конструирования чат-ботов какие-то дополнительные источники информации. Будущий специалист создает и интегрирует чат-бот, осуществляет базовые настройки приватности при незначительной помощи преподавателя.

Конструктор (от 80 до 90 баллов) – студент знает и понимает все риски, проблемы и тенденции в области обеспечения информационной безопасности. Он самостоятелен в поиске вспомогательных источников информации для выполнения заданий в виртуальной среде. Будущий специалист без помощи преподавателя конструирует чат-бот, интегрирует его в сообщество, осуществляет базовые и дополнительные настройки приватности.

На втором этапе исследования студенты работали с чат-ботами согласно описанной ранее логике информационного взаимодействия. Будущие специалисты из контрольной группы изучали те же самые теоретические вопросы и темы, цифровые сервисы, что и участники экспериментальной группы. Однако к организованной деятельности по конструированию чат-ботов и применению их для изучения дополнительных аспектов кибербезопасности не привлекались. На фиксирующей стадии ОЭР еще раз проводилась контрольная работа, содержащая 60 заданий.

В Таблице ниже представлены результаты анализа уровней подготовки специалистов по информационной безопасности до и после конструирования чат-ботов.

Уровень подготовки специалистов

Уровень	Группы			
	Экспериментальная группа (42 студента)		Контрольная группа (42 студента)	
	До эксперимента	После эксперимента	До эксперимента	После эксперимента
Наблюдатель	48% (20)	24% (10)	45% (19)	42% (18)
Испытатель	42% (18)	48% (20)	45% (19)	48% (20)
Конструктор	10% (4)	28% (12)	10% (4)	10% (4)

Для $\alpha = 0,05$ по таблицам распределения χ^2 крит равно 5,991. Таким образом, вычисляем: $\chi^2_{\text{набл.1}} < \chi^2_{\text{крит}}$ ($0,053 < 5,991$), а $\chi^2_{\text{набл.2}} > \chi^2_{\text{крит}}$ ($6,286 > 5,991$). Следовательно, изменения в уровнях подготовки не являются случайными.

Заключение / Conclusion

В материалах статьи авторами описана работа студентов, обучающихся по направлению подготовки 10.03.01 «Информационная безопасность автоматизированных систем». Конструирование чат-ботов выполнено по следующим этапам: изучение возможностей сервиса, интерфейса и базовых инструментов виртуальной среды; создание первого чат-бота по инструкции; разработка и защита собственного чат-бота по направлению подготовки.

Результаты исследования позволили выявить следующие особенности применения сервисов по конструированию чат-ботов в обучении специалистов по информационной безопасности:

- 1) необходимо на всех этапах взаимодействия создавать условия для понимания обучающимися важности профессии в области IT и защиты информации;
- 2) изучение инструментов ИИ и конструирование чат-ботов в виртуальной среде должно находиться во взаимосвязи с изучением других цифровых технологий (3D-моделирование, программирование и др.);

3) формирование представлений обучающихся о рисках, этических проблемах интеграции элементов ИИ в конструирование чат-ботов с последующим обсуждением этих аспектов;

4) учет специфических проблем кибербезопасности в контексте появления новых угроз и атак (правила для ботов социальной сети «ВКонтакте», несанкционированный доступ к информации, нарушение приватности персональных данных, дезинформация).

Полученные результаты могут быть использованы для совершенствования программ подготовки ИТ-специалистов, реализуемых на базе РТУ МИРЭА (ИКБ).

Ссылки на источники / References

1. Guidance for generative AI in education and research. – URL: <https://www.unesco.org/en/articles/guidance-generative-ai-education-and-research>
2. The Digital Innovation Summit Bucharest 2025. – URL: <https://www.thediplomat.ro/2025/03/12/digital-innovation-summit-bucharest-disb-2025-building-a-secure-and-resilient-digital-future-together/>
3. Национальная стратегия развития ИИ на период до 2030 года // Указ Президента РФ от 10.10.2019 № 490. – URL: <https://ai.gov.ru/national-strategy/>
4. Институт образования НИУ ВШЭ. – URL: <https://www.hse.ru/news/priority/1010385434.html>
5. Тронь Т. А. Современное состояние и проблемы подготовки специалистов по информационной безопасности в системе среднего профессионального образования // Профессиональное педагогическое образование в логике глобальных трансформационных процессов: проблемы и пути решения: сб. материалов Всерос. науч.-практ. конф. с междунар. участием, посвящ. 80-летию А. В. Ивановой, Якутск, 03 октября 2025 года. – Киров: Межрегиональный центр инновационных технологий в образовании, 2025. – С. 16–19.
6. Hanshaw G., Sullivan C. Exploring barriers to AI course assistant adoption: a mixed-methods study on student non-utilization // Discover Artificial Intelligence. – 2025. – Vol. 5. – P. 1–24. – DOI: 10.1007/s44163-025-00312-x.
7. Thoeni A., Fryer L. AI Chatbots in Higher Education: Comparing Expectations to Evidence // Computers in Human Behavior Reports. – 2026. – Vol. 22. – P. 101061. – DOI: 10.1016/j.chbr.2026.101061.
8. Ezekwem C., Ucheji C., Ekeneme J. C. AI Readiness in National Cybersecurity Strategies: A Cross-Country Comparative Study // International Journal of Research and Innovation in Applied Science. – 2025. – Vol. 10. – P. 839–846. – DOI: 10.51584/IJRIAS.2025.1010000067.
9. Arkhipova A. Methodology of Decision-Making in Information Security Specialist Training Management Systems // AISMA 2025. Lecture Notes in Networks and Systems. – 2026. – Vol. 1456. – DOI: https://doi.org/10.1007/978-3-032-07275-7_5
10. Reznichenko M., Pomelnikova E. Professional successfulness of information security specialists // Vestnik of Samara University. History, pedagogics, philology. – 2019. – Vol. 25. – P. 82. – DOI: 10.18287/2542-0445-2019-25-3-82-88.
11. Swapna S., Sivalingam V. AI Integration and Its Impact on Cyber Defense: A Theoretical Analysis // International Journal of Information Security and Cybercrime. – 2025. – Vol. XIV(1). – P. 76–87. – DOI: 10.19107/IJISC.2025.01.05
12. Shchedrina E. V., Soboleva E. V., Ivashova O. N. Development of students' systems thinking when studying the basics of artificial intelligence in engineering practice at the agricultural university // Perspectives of Science and Education. – 2026. – No. 2(80). – P. 131–145. – DOI: 10.32744/pse.2026.2.7.
13. Supangkat F., Ramadhani O., Putranto R., Albana I. Analisis peran kecerdasan buatan dalam meningkatkan keamanan data di era digital // Jurnal Mahasiswa Sistem Informasi (JMSI). – 2025. – Vol. 6. – P. 159–169. – DOI: 10.24127/jmsi.v6i2.8982.
14. Ifelebuegu A., Kulume P., Cherukut P. Chatbots and AI in Education (AIEd) tools: The good, the bad, and the ugly // Journal of Applied Learning & Teaching. – 2023. – Vol. 6. – P. 1–14. – DOI: 10.37074/jalt.2023.6.2.29.
15. Amin M., Rasyid H., Akmal A. AHP – Saw decision support system for AI-based teaching material recommendation // Jurteksi. – 2026. – Vol. 12. – P. 399–406. – DOI: 10.33330/jurteksi.v12i2.4537.
16. Binhammad M., Othman A., Abuljadayel L. et al. Investigating Advanced Generative Dialogue Systems for Educational Chatbots // Creative Education. – 2024. – Vol. 15. – P. 1593–1626. – DOI: 10.4236/ce.2024.158096.
17. Wiboolyasarin W., Wiboolyasarin K., Tiranant P. et al. AI-driven chatbots in second language education: A systematic review of their efficacy and pedagogical implications // Ampersand. – 2025. – Vol. 14. – P. 100224. – DOI: 10.1016/j.amper.2025.100224.
18. Pikhart M., Al-Obaydi L. Reporting the potential risk of using AI in higher Education: Subjective perspectives of educators // Computers in Human Behavior Reports. – 2025. – Vol. 18. – DOI: 10.1016/j.chbr.2025.100693.
19. Gilbert C., Gilbert M. Leveraging Artificial Intelligence (AI) by a Strategic Defense against Deepfakes and Digital Misinformation // International Journal of Scientific Research and Modern Technology (IJSRMT). – 2024. – Vol. 3. – P. 62–78. – DOI: 10.38124/ijsrmt.v3i11.76.

20. Simos C., Tzagkourni E., Bardis N., Doukas N. The transformation of STEM education through educational chatbots and digital technologies // *Global Journal of Engineering and Technology Advances*. – 2026. – Vol. 26. – P. 181–194. – DOI: 10.30574/gjeta.2026.26.3.0067.
 21. Jamaludin J., Leasa M., Rachman G. et al. Enhancing Middle School Teachers' Understanding of Locally Context-Based STEM Learning // *Unram Journal of Community Service*. – 2025. – Vol. 7. – P. 137–146. – DOI: 10.29303/ujcs.v7i1.1616.
 22. Developing the emotional intelligence of teachers working with gifted children when designing educational chatbots / E. V. Soboleva, T. N. Suvorova, L. A. Shunina, P. M. Gorev // *Perspectives of Science and Education*. – 2025. – No. 6(78). – P. 624–637. – DOI 10.32744/pse.2025.6.41.
 23. Ploybut S. Management of AI Chatbots in Education: A Systematic Literature Review // *Journal of Management Science Sakon Nakhon Rajabhat University*. – 2026. – Vol. 5(4). – P. 1655–1669. – URL: <https://so08.tci-thaijo.org/index.php/JMSSNRU/article/view/5294>
 24. Sharma V., Sehrawat Dr., Verma M. et al. A comprehensive analysis of the role and impact of chatbots in higher education // *Archives for Technical Sciences*. – 2025. – Vol. 2. – P. 700–708. – DOI: 10.70102/afts.2025.1833.700.
 25. Roy V. I., Janardhanan K. A. Exploring the Relationship Between Teacher Job Satisfaction, Self-Efficacy, and Student Engagement in Engineering Classrooms // *Indian Journal of Information Sources and Services*. – 2025. – Vol. 15. – P. 107–114. – DOI: 10.51983/ijiss-2025.IJISS.15.1.15.
 26. Kumar R., Ajeet K., Rai. The Impact of AI-Powered Chatbots on Self-Regulated Learning in Higher Education // *A Quarterly Multidisciplinary Blind Peer Reviewed & Refereed Online International Journal*. – 2026. – Vol. (3). – Issue (1). – P. 383–388. – DOI: 10.5281/zenodo.19211570.
 27. Wibowo F., Hasbey H., Aziz T. et al. Integrating artificial intelligence chatbot climate change with physics digital modules for student learning assistants // *Multidisciplinary Science Journal*. – 2025. – Vol. 7. – P. 1–14. – DOI: 10.31893/multiscience.2025583.
 28. Anvitha K., Durjay T., Sathvika K. et al. EduBot: A Compact AI-Driven Study Assistant for Contextual Knowledge Retrieval // *2025 Global Conference in Emerging Technology (GINOTECH)*. – 2025. – P. 1–7. – DOI: 10.1109/GINOTECH63460.2025.11077097.
 29. Hanshaw G., Sullivan C. Exploring barriers to AI course assistant adoption: a mixed-methods study on student non-utilization.
 30. Варламов А. С. Обзор технологий, применяемых в интеллектуальных диалоговых системах // *Вестник Воронежского государственного университета. Серия: Системный анализ и информационные технологии*. – 2025. – № 2. – С. 139–156. – DOI: 10.17308/sait/1995-5499/2025/2/139-156.
 31. Смык А. Ф., Гусева Е. А. Искусственный интеллект в образовании будущих инженеров: фокус на предметной области // *Инженерное образование*. – 2025. – № 38. – С. 205–221. – DOI: 10.54835/18102883_2025_38_18.
 32. Быков А. А., Киселева О. М. Оценка эффективности применения чат-бота как информационной поддержки преподаваемой дисциплины // *Современные проблемы науки и образования*. – 2022. – № 1. – С. 34. – DOI: 10.17513/spno.31481.
 33. Бойправ О. В., Клиндухов Я. А., Мажаева С. Д. Применение обучающих игр для формирования специальных навыков по защите от угроз информационной безопасности // *Технические средства защиты информации: материалы XXIV Междунар. науч.-техн. конф., Минск, 08 апреля 2026 года*. – Минск: БГУИР, 2026. – С. 44–49.
 34. Подготовка специалистов по безопасности к противодействию вредоносным веб-ботам / Н. Худер, П. И. Сигети, И. Б. Государев, М. Альжниди // *Современное образование: традиции и инновации*. – 2024. – № 4. – С. 77–81. – DOI: 10.51623/23132027.2404.08.
-
1. *Guidance for generative AI in education and research*. Available at: <https://www.unesco.org/en/articles/guidance-generative-ai-education-and-research> (in English).
 2. *The Digital Innovation Summit Bucharest 2025*. Available at: <https://www.thediplomat.ro/2025/03/12/digital-innovation-summit-bucharest-disb-2025-building-a-secure-and-resilient-digital-future-together/> (in English).
 3. “Nacional'naya strategiya razvitiya II na period do 2030 goda” [National AI Development Strategy for the Period up to 2030], *Ukaz Prezidenta RF ot 10.10.2019 № 490*. Available at: <https://ai.gov.ru/national-strategy/> (in Russian).
 4. *Institut obrazovaniya NIU VShE [HSE Institute of Education]*. Available at: <https://www.hse.ru/news/priority/1010385434.html> (in Russian).
 5. Tron', T. A. (2025). “Sovremennoe sostoyanie i problemy podgotovki specialistov po informacionnoj bezopasnosti v sisteme srednee professional'noe obrazovanie” [Current Condition and Challenges of Training Information Security Specialists within the Secondary Vocational Education System], *Professional'noe pedagogicheskoe obrazovanie v logike global'nyh transformacionnyh processov: problemy i puti resheniya: sb. materialov Vseros. nauch.-prakt. konf. s mezhdunar. uchastiem, posvyashch. 80-letiyu A. V. Ivanovoj, Yakutsk, 03 oktyabrya 2025 goda, Mezhhregional'nyj centr innovacionnyh tekhnologij v obrazovanii, Kirov*, pp. 16–19 (in Russian).
 6. Hanshaw, G., & Sullivan, C. (2025). “Exploring barriers to AI course assistant adoption: a mixed-methods study on student non-utilization”, *Discover Artificial Intelligence*, vol. 5, pp. 1–24. DOI: 10.1007/s44163-025-00312-x (in English).

7. Thoeni, A., & Fryer, L. (2026). "AI Chatbots in Higher Education: Comparing Expectations to Evidence", *Computers in Human Behavior Reports*, vol. 22, p. 101061. DOI: 10.1016/j.chbr.2026.101061 (in English).
8. Ezekwem, C., Ucheji, C., & Ekeneme, J. C. (2025). "AI Readiness in National Cybersecurity Strategies: A Cross-Country Comparative Study", *International Journal of Research and Innovation in Applied Science*, vol. 10, pp. 839–846. DOI: 10.51584/IJRIAS.2025.1010000067 (in English).
9. Arkhipova, A. (2026). "Methodology of Decision-Making in Information Security Specialist Training Management Systems", *AISMA 2025. Lecture Notes in Networks and Systems*, vol. 1456. DOI: https://doi.org/10.1007/978-3-032-07275-7_5 (in English).
10. Reznichenko, M., & Pomelnikova, E. (2019). "Professional successfulness of information security specialists", *Vestnik of Samara University. History, pedagogics, philology*, vol. 25, p. 82. DOI: 10.18287/2542-0445-2019-25-3-82-88 (in English).
11. Swapna, S., & Sivalingam, V. (2025). "AI Integration and Its Impact on Cyber Defense: A Theoretical Analysis", *International Journal of Information Security and Cybercrime*, vol. XIV(1), pp. 76–87. DOI: 10.19107/IJISC.2025.01.05 (in English).
12. Shchedrina, E. V., Soboleva, E. V., & Ivashova, O. N. (2026). "Development of students' systems thinking when studying the basics of artificial intelligence in engineering practice at the agricultural university", *Perspectives of Science and Education*, no. 2(80), pp. 131–145. DOI: 10.32744/pse.2026.2.7 (in English).
13. Supangkat, F., Ramadhani, O., Putranto, R., & Albana, I. (2025). "Analisis peran kecerdasan buatan dalam meningkatkan keamanan data di era digital" [An analysis of the role of artificial intelligence in enhancing data security in the digital era], *Jurnal Mahasiswa Sistem Informasi (JMSI)*, vol. 6, pp. 159–169. DOI: 10.24127/jmsi.v6i2.8982 (in Indonesian).
14. Ifelebuegu, A., Kulume, P., & Cherukut, P. (2023). "Chatbots and AI in Education (AIEd) tools: The good, the bad, and the ugly", *Journal of Applied Learning & Teaching*, vol. 6, pp. 1–14. DOI: 10.37074/jalt.2023.6.2.29 (in English).
15. Amin, M., Rasyid, H., & Akmal, A. (2026). "AHP – Saw decision support system for AI-based teaching material recommendation", *Jurteks*, vol. 12, pp. 399–406. DOI: 10.33330/jurteks.v12i2.4537 (in English).
16. Binhammad, M., Othman, A., Abuljadayel, L. et al. (2024). "Investigating Advanced Generative Dialogue Systems for Educational Chatbots", *Creative Education*, vol. 15, pp. 1593–1626. DOI: 10.4236/ce.2024.158096 (in English).
17. Wiboolyasarin, W., Wiboolyasarin, K., Tiranant, P. et al. (2025). "AI-driven chatbots in second language education: A systematic review of their efficacy and pedagogical implications", *Ampersand*, vol. 14, p. 100224. DOI: 10.1016/j.amper.2025.100224 (in English).
18. Pikhart, M., & Al-Obaydi, L. (2025). "Reporting the potential risk of using AI in higher Education: Subjective perspectives of educators", *Computers in Human Behavior Reports*, vol. 18. DOI: 10.1016/j.chbr.2025.100693 (in English).
19. Gilbert, C., & Gilbert, M. (2024). "Leveraging Artificial Intelligence (AI) by a Strategic Defense against Deepfakes and Digital Misinformation", *International Journal of Scientific Research and Modern Technology (IJSRMT)*, vol. 3, pp. 62–78. DOI: 10.38124/ijsrmt.v3i11.76 (in English).
20. Simos, C., Tzagakourni, E., Bardis, N., & Doukas, N. (2026). "The transformation of STEM education through educational chatbots and digital technologies", *Global Journal of Engineering and Technology Advances*, vol. 26, pp. 181–194. DOI: 10.30574/gjeta.2026.26.3.0067 (in English).
21. Jamaludin, J., Leasa, M., Rachman, G. et al. (2025). "Enhancing Middle School Teachers' Understanding of Locally Context-Based STEM Learning", *Unram Journal of Community Service*, vol. 7, pp. 137–146. DOI: 10.29303/ujcs.v7i1.1616 (in English).
22. Soboleva, E. V., Suvorova, T. N., Shunina, L. A., & Gorev, P. M. (2025). "Developing the emotional intelligence of teachers working with gifted children when designing educational chat-bots", *Perspectives of Science and Education*, no. 6(78), pp. 624–637. DOI: 10.32744/pse.2025.6.41 (in English).
23. Ploybut, S. (2026). "Management of AI Chatbots in Education: A Systematic Literature Review", *Journal of Management Science Sakon Nakhon Rajabhat University*, vol. 5(4), pp. 1655–1669. Available at: <https://so08.tci-thaijo.org/index.php/JMSSNRU/article/view/5294> (in English).
24. Sharma, V., Sehrawat, Dr., Verma, M. et al. (2025). "A comprehensive analysis of the role and impact of chatbots in higher education", *Archives for Technical Sciences*, vol. 2, pp. 700–708. DOI: 10.70102/afts.2025.1833.700 (in English).
25. Roy, V. I., & Janardhanan, K. A. (2025). "Exploring the Relationship Between Teacher Job Satisfaction, Self-Efficacy, and Student Engagement in Engineering Classrooms", *Indian Journal of Information Sources and Services*, vol. 15, pp. 107–114. DOI: 10.51983/ijiss-2025.IJISS.15.1.15 (in English).
26. Kumar, R., Ajeet, K., & Rai. (2026). "The Impact of AI-Powered Chatbots on Self-Regulated Learning in Higher Education", *A Quarterly Multidisciplinary Blind Peer Reviewed & Refereed Online International Journal*, vol. (3), issue (1), pp. 383–388. DOI: 10.5281/zenodo.19211570 (in English).
27. Wibowo, F., Hasbey, H., Aziz, T. et al. (2025). "Integrating artificial intelligence chatbot climate change with physics digital modules for student learning assistants", *Multidisciplinary Science Journal*, vol. 7, pp. 1–14. DOI: 10.31893/multiscience.2025583 (in English).
28. Anvitha, K., Durjay, T., Sathvika, K. et al. (2025). "EduBot: A Compact AI-Driven Study Assistant for Contextual Knowledge Retrieval", *2025 Global Conference in Emerging Technology (GINOTECH)*, pp. 1–7. DOI: 10.1109/GINOTECH63460.2025.11077097 (in English).

29. Hanshaw, G., & Sullivan, C. (2025). Op. cit.
30. Varlamov, A. S. (2025). "Obzor tekhnologii, primenyaemyh v intellektual'nyh dialogovyh sistemah" [Overview of technologies used in intelligent dialogue systems], *Vestnik Voronezhskogo gosudarstvennogo universiteta. Seriya: Sistemnyy analiz i informacionnye tekhnologii*, № 2, pp. 139-156. DOI: 10.17308/sait/1995-5499/2025/2/139-156 (in Russian).
31. Smyk, A. F., & Guseva, E. A. (2025). "Iskusstvennyj intellekt v obrazovanii budushchih inzhenerov: fokus na predmetnoj oblasti" [Artificial Intelligence in the Education of Future Engineers: A Focus on the Subject Domain], *Inzhenernoe obrazovanie*, № 38, pp. 205–221. DOI: 10.54835/18102883_2025_38_18 (in Russian).
32. Bykov, A. A., & Kiseleva, O. M. (2022). "Ocenka effektivnosti primeneniya chat-bota kak informacionnoj podderzhki prepodavaemoj discipliny" [Assessing the effectiveness of using a chatbot to provide information support for a taught course], *Sovremennye problemy nauki i obrazovaniya*, № 1, p. 34. DOI: 10.17513/spno.31481 (in Russian).
33. Bojprav, O. V., Klinduhov, Ya. A., & Mazhaeva, S. D. (2026). "Primenenie obuchayushchih igr dlya formirovaniya special'nyh navykov po zashchite ot ugroz informacionnoj bezopasnosti" [The Use of Educational Games to Develop Specialized Skills for Protection Against Information Security Threats], *Tekhnicheskie sredstva zashchity informacii: materialy HXIV Mezhdunar. nauch.-tekhn. konf., Minsk, 08 aprelya 2026 goda*, BGUIR, Minsk, pp. 44–49 (in Russian).
34. Huder, N. et al. (2024). "Podgotovka specialistov po bezopasnosti k protivodejstviyu vredonosnym veb-botam" [Training security professionals to counter malicious web bots], *Sovremennoe obrazovanie: tradicii i innovacii*, № 4, pp. 77–81. DOI: 10.51623/23132027.2404.08 (in Russian).

Вклад авторов

З. В. Шилова – активное участие в разработке содержания дисциплины «Информатика» для обучения студентов программы подготовки 10.03.01 «Информационная безопасность автоматизированных систем». На заключительном этапе – формулировка выводов по исследованию.

Н. А. Елизарова – преподавание дисциплины «Информатика»; анализ российской и зарубежной литературы по проблематике исследования, описание методологии, обработка экспериментальных данных.

Н. И. Ивахненко – при работе над текстом статьи проанализированы зарубежные источники, баз данных Scopus и WoS; оформление аналитических материалов соавторов согласно структуре статьи, выполнение статистической обработки результатов.

Contribution of the authors

Z. V. Shilova – active participation in developing the content of the "Informatics" course for students in the "Information Security of Automated Systems" program (code 10.03.01); formulation of research conclusions.

N. A. Elizarova – teaching the "Informatics" course; analysis of Russian and international literature relevant to the research topic; description of the methodology; processing of experimental data.

N. I. Ivakhnenko – analysis of international sources and databases (Scopus and Web of Science) during the drafting of the article; formatting of co-authors' analytical materials in accordance with the article's structure; statistical processing of the results.