RUDN Journal of Informatization in Education
Вестник РУДН. Серия: Информатизация образования
ISSN 2312-8631 (Print); ISSN 2312-864X (Online)
2026 Vol. 23 No. 2 221–232
http://journals.rudn.ru/nformatization-education

DOI: 10.22363/2312-8631-2026-23-2-221-232
EDN: RTXDWA
УДК 378.147.88

Научная статья / Research article

Возможности применения виртуальной инженерно-технической лаборатории в практической подготовке специалистов по информационной безопасности

М.В. Тумбинская ✉, Б.И. Гатауллин, Э.И. Хаерова

Казанский национальный исследовательский технический университет им. А.Н. Туполева – КАИ, Казань, Российская Федерация
✉tumbinskaya@inbox.ru

Аннотация. *Постановка проблемы.* Информатизация образования, внедрение инновационных образовательных технологий, в том числе технологий виртуальной и дополненной реальности, открывают новые возможности для повышения качества обучения. Использование виртуальных тренажеров и симуляторов позволяет моделировать сложные системы и реалистичные сценарии, способствуя формированию практических навыков и компетенций в условиях, максимально приближенных к реальным. Особую актуальность в подготовке специалистов по инженерно-технической защите информации, где традиционные формы практического обучения ограничены, приобретает внедрение виртуальных тренажеров и лабораторий, имитирующих работу с современными системами защиты в безопасной и контролируемой среде. Цель исследования – повышение качества подготовки специалистов в области защиты информации за счет разработки и практического применения виртуальной инженерно-технической лаборатории, позволяющей имитировать решение реальных профессиональных задач. *Методология.* Проблема рассмотрена на примере раздела «Инженерно-техническая защита информации» дисциплины «Защита информации». Апробация проведена на базе Казанского национального исследовательского технического университета им. А.Н. Туполева – КАИ со студентами направления 09.03.03 «Прикладная информатика». Обучающимся предлагалось смоделировать систему защиты информации для заданного объекта по следующим направлениям: защита от утечек по техническим каналам; безопасность сетей и систем передачи данных; применение средств охранной и пожарной сигнализации как элементов физической и инженерно-технической безопасности. *Результаты.* В процессе изучения раздела «Инженерно-техническая защита информации» проведена сравнительная оценка качества обучения двух групп студентов: первая использовала виртуальную лабораторию в сочетании с традиционными методическими указаниями, вторая – только традиционные материалы. Применение виртуальной лаборатории позволило повысить качество обучения за счет увеличения точности решения задач, сокращения временных затрат

на выполнение кейсов и снижения частоты ошибок. *Заключение*. Возможности применения виртуальной инженерно-технической лаборатории в практической подготовке специалистов по информационной безопасности подтверждает целесообразность ее использования для решения реальных задач инженерно-технической защиты информации.

Ключевые слова: виртуальный тренажер, технические средства защиты информации, информатизация образования, объект информатизации, виртуальная реальность

Вклад авторов. *М.В. Тумбинская* – концепция (формулирование идеи, целей и задач), дизайн, разработка методологии, создание модели исследования, написание рукописи. *Б.И. Гатауллин* – разработка программного обеспечения, реализация компьютерного кода и вспомогательных алгоритмов, тестирование существующих компонентов кода, предоставление ресурсов. *Э.И. Хаерова* – сбор, верификация, анализ, синтез, администрирование и визуализация данных исследования, проведение экспериментов, редактирование рукописи. Все авторы прочли и одобрили окончательную версию рукописи.

Заявление о конфликте интересов. Авторы заявляют об отсутствии конфликта интересов.

История статьи: поступила в редакцию 24 июня 2025 г.; доработана после рецензирования 19 ноября 2025 г.; принята к публикации 24 февраля 2026 г.

Для цитирования: *Тумбинская М.В., Гатауллин Б.И., Хаерова Э.И.* Возможности применения виртуальной инженерно-технической лаборатории в практической подготовке специалистов по информационной безопасности // Вестник Российского университета дружбы народов. Серия: Информатизация образования. 2026. Т. 23. № 2. С. 221–232. http://doi.org/10.22363/2312-8631-2026-23-2-221-232 EDN: RTXDWA

The possibilities of using a virtual engineering laboratory in the practical training of information security specialists

Marina V. Tumbinskaya ✉, Bulat I. Gataullin, Endzhe I. Haerova

Kazan National Research Technical University named after A.N. Tupolev – KAI, Kazan, Russian Federation
✉tumbinskaya@inbox.ru

Abstract. *Problem statement.* In the modern education system, special attention is paid to the formation of professional competencies. Informatization of education and the introduction of innovative educational technologies, including virtual and augmented reality technologies, open up new opportunities for improving the quality of education. The use of virtual simulators and simulators allows you to simulate complex cyber-physical systems and realistic scenarios, contributing to the formation of practical skills and competencies in conditions as close as possible to real ones. Of particular relevance in the training of specialists in engineering and technical information protection, where traditional forms of practical training are limited, is the introduction of virtual simulators and laboratories that simulate working with modern security systems in a secure and controlled environment. The purpose of the research is to improve the quality of training specialists in the field of information security through the development and practical application of a virtual engineering laboratory that allows simulating the solution of

real professional tasks. *Methodology.* The problem is considered using the example of the section "Engineering and technical information protection" of the discipline "Information Protection". The approbation was carried out on the basis of Kazan National Research Technical University named after A.N. Tupolev – KAI with students of the direction 09.03.03 "Applied Informatics". Students were asked to model an information security system for a given facility in the following areas: protection against leaks through technical channels; security of networks and data transmission systems; the use of security and fire alarm systems as elements of physical and engineering safety. *Results.* In the process of studying the section "Engineering and technical information protection", a comparative assessment of the quality of education of two groups of students was carried out: the first used a virtual laboratory in combination with traditional methodological guidelines, the second used only traditional materials. The use of a virtual laboratory has improved the quality of training by increasing the accuracy of solving problems, reducing the time required to complete cases and reducing the error rate. *Conclusion.* The possibility of using a virtual engineering laboratory in the practical training of information security specialists confirms the expediency of its use to solve real problems of engineering and technical information protection.

Keywords: virtual simulator, technical means of information protection, informatization of education, object of informatization, virtual reality

Authors' contribution. *M.V. Tumbinskaya* – concept (formulation of the idea, goals, and objectives), design, methodology development, creation of the research model, manuscript writing. *B.I. Gataullin* – software development, implementation of the computer code and auxiliary algorithms, testing of existing code components, provision of resources. *E.I. Haerova* – data verification, analysis and synthesis of research data, conduct of experiments, data collection, data administration and visualization, editing of the manuscript. All authors have read and approved the final version of the manuscript.

Conflict of interest. The authors declare that there is no conflict of interest.

Article history: received 24 June 2025; revised 19 November 2025; accepted 24 February 2026.

For citation: Tumbinskaya MV, Gataullin BI, Haerova EI. The possibilities of using a virtual engineering laboratory in the practical training of information security specialists. *RUDN Journal of Informatization in Education.* 2026;23(2):221–232. (In Russ.) http://doi.org/10.22363/2312-8631-2026-23-2-221-232 EDN: RTXDWA

Постановка проблемы. В современной системе образования особое внимание уделяется формированию профессиональных компетенций. Информатизация образовательного процесса и интеграция инновационных цифровых технологий, таких как средства виртуальной и дополненной реальности, открывают новые возможности для повышения качества обучения. Применение виртуальных тренажеров и иммерсивных сред позволяет моделировать сценарии решения профессиональных задач в условиях, максимально приближенных к реальным [1–3].

Особую актуальность данный подход приобретает в подготовке специалистов в области инженерно-технической защиты информации, где традиционные формы практического обучения имеют ряд ограничений. Например, организационные ограничения связаны с обеспечением доступа к реальным объектам (предприятиям, критически важным инфраструктурам

и др.), материально-технические – недостаточным оснащением специализированных лабораторий современными средствами защиты информации (ЗИ) и др. Реализация данного подхода способствует развитию и формированию практических компетенций, необходимых для профессиональной деятельности. Цель исследования – повышение качества подготовки специалистов в области ЗИ за счет разработки и практического применения виртуальной инженерно-технической лаборатории, позволяющей имитировать решение реальных профессиональных задач.

Методология. Анализ литературных источников [4–8] свидетельствует о наличии виртуальных тренажеров, моделирующих системы инженерно-технической ЗИ, включая контроль доступа, видеонаблюдение, охранно-пожарную сигнализацию, защиту периметра и противодействие утечкам по техническим каналам объекта информатизации. Под объектом информатизации понимается совокупность физических помещений и информационных ресурсов, подлежащих защите от внутренних и внешних угроз информационной безопасности (ИБ). Для достижения цели исследования использовались методы системного анализа, моделирования и проектирования, программной реализации, эксперимент, а также статистической обработки данных.

Предлагается программное обеспечение – виртуальная лаборатория, предназначенная для имитации решения реальных профессиональных задач на примере раздела «Инженерно-техническая защита информации» дисциплины «Защита информации». Студентам было предложено смоделировать систему защиты объекта по направлениям: противодействие утечкам по техническим каналам; безопасность сетей передачи данных; применение средств охранно-пожарной сигнализации в рамках физической и инженерно-технической защиты.

Результаты и обсуждение. Разработка программного обеспечения – виртуальной лаборатории осуществлялась в среде Unity с использованием языка C#. В процессе разработки применялся итеративный подход, включающий циклы тестирования и отладки на локальной машине Lenovo Ideapad 310-15ISK с x64-архитектурой. Конфигурация тестового оборудования включала процессор Intel® Core™ i5-6200U (2,30 ГГц, 2 ядра, 4 логических процессора). Виртуальная лаборатория моделирует объект информатизации, позволяя пользователям:

1) интерактивно отрабатывать методы обнаружения уязвимостей;

2) осваивать установку и настройку технических средств защиты информации (ТСЗИ).

В основу программного обеспечения заложены модели ТСЗИ: ФЭПС-10, SEL SP-157 «Шагрень», SEL SP-157VP, SEL SP-157VPS, SEL SP-157AS, МП-8 «Сигма-РА», комплект системы контроля доступа (СКУД) ATIS № 4 с электромагнитным замком и бесконтактной кнопкой выхода, а также IP-камера видеонаблюдения ST-183M IP STARLIGHT H.265 [9–14]. Эти средства являются инструментами для формирования компетенций обучаемых при решении задач инженерно-технической ЗИ. На программный код виртуальной лаборато-

рии получено свидетельство о государственной регистрации программы для ЭВМ № 2025666993[1].

Алгоритм взаимодействия обучаемого с программным обеспечением состоит из определенных шагов.

1. Погружение в виртуальную среду офиса.
2. Анализ уязвимостей – обследование инфраструктуры на наличие угроз ИБ.
3. Выбор и изучение ТСЗИ.
4. Подготовка и установка – перенос в активную зону, выбор точек размещения и фиксация ТСЗИ.
5. Цикл – шаги 3–4 повторяются для всех необходимых средств.
6. Проверка и коррекция результата, исправление ошибок.
7. Завершение – задание считается выполненным после успешной проверки.

Экспериментальное исследование. Исследование проводилось в три этапа в течение 4 месяцев на базе Казанского национального исследовательского технического университета им. А.Н. Туполева – КАИ. В эксперименте участвовали 42 обучающихся направления 09.03.03 «Прикладная информатика» (средний возраст – 21 год; 12 % девушек, 88 % юношей).

На первом этапе определялся исходный уровень теоретических знаний и компетенций студентов в области инженерно-технической ЗИ, а также интерес к данной предметной области. Опрос респондентов осуществлялся с использованием средств Yandex Forms по следующим блокам: самооценка уровня цифровых компетенций; наличие практического опыта работы с ТСЗИ; знание правил установки ТСЗИ; знание правил размещения оборудования в серверной стойке; интерес к технической ЗИ. Анализ результатов исследования первого этапа показал, что 78 % респондентов знакомы с некоторыми видами ТСЗИ, но лишь 12 % имеют практический опыт, 67 % студентов затруднились оценить свой уровень знаний по правилам установки ТСЗИ и правилам размещения оборудования в серверной стойке. У 83 % респондентов имеется интерес к технической защите информации. Следовательно, внедрение виртуальной лаборатории в учебный процесс может повысить качество обучения за счет реализации активных, имитационных форм, способствующих формированию практических компетенций в условиях, приближенных к профессиональной деятельности.

В рамках второго этапа экспериментального исследования использовались:

1) разработанное программное обеспечение – виртуальная лаборатория;

2) методические материалы, включающие практические задания по выявлению угроз и каналов утечки информации, кейсы по моделированию системы ЗИ с размещением средств защиты на ситуационном плане объекта информатизации.

[1] Патент RU 2025667813. Виртуальная инженерно-техническая лаборатория защиты информации : № 2025666993 : заявл. 09.07.2025 : опубл. 09.07.2025 / Гатауллин Б.И., Хаерова Э.И., Тумбинская М.В. EDN: VIVKTX

Рассмотрим пример кейса. Кейс представляет собой моделируемый процесс выбора и размещения ТСЗИ в виртуальной среде с последующей проверкой.

1. Выбор сценария. Студент запускает лабораторию и выбирает одно из трех виртуальных пространств для моделирования:

- инженерно-техническая защита информации – офисное помещение, в котором вращается конфиденциальная информация;
- сети и системы передачи данных – сетевая инфраструктура офиса;
- охранная и пожарная сигнализация – периметр и внутренние помещения объекта.

2. Размещение средств защиты. Студент анализирует угрозы, каналы утечки информации и выбирает необходимые ТСЗИ из каталога. Требуется корректно разместить выбранные средства (например, камеры, датчики) на виртуальном объекте. На рисунках 1–3 показаны интерфейсные формы пространства виртуальной лаборатории «Инженерно-техническая защита информации».

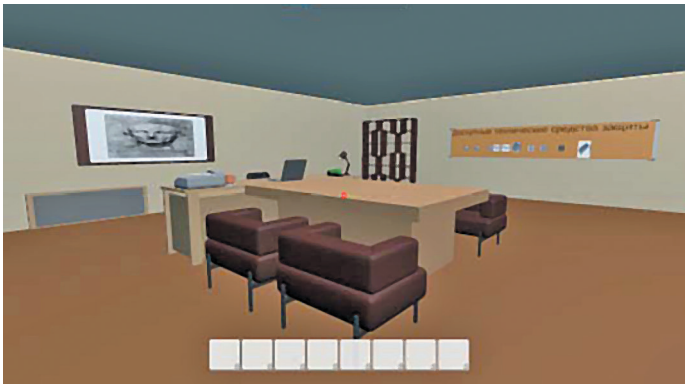

Рис. 1. Интерфейсная часть диалогового окна пространства виртуальной лаборатории «Инженерно-техническая защита информации»

Источник: создано М.В. Тумбинской, Б.И. Гатауллиным, Э.И. Хаеровой.

Figure 1. The interface part of the dialog box of the virtual laboratory space *Engineering and Technical Information Protection*

Source: created by Marina V. Tumbinskaya, Bulat I. Gataullin, Endzhe I. Haerova.

3. Проверка решения. Система автоматически проверяет результат по параметрам:

- полнота покрытия – защищены ли все критические зоны;
- соответствие стандартам – соблюдены ли нормативы ГОСТ Р 52435-2015, ГОСТ Р 56627-2015, ГОСТ Р 57142-2016 (зоны контроля, расстояния и т.д.);
- отсутствие конфликтов – корректно ли взаимодействуют средства между собой;
- обратная связь – «Успех» – правильно установленные ТСЗИ подсвечиваются зеленым; «Неудача» – ошибочные элементы выделяются красным с подсказками по исправлению.

Студент итеративно вносит коррективы и повторяет проверку до полного устранения ошибок.

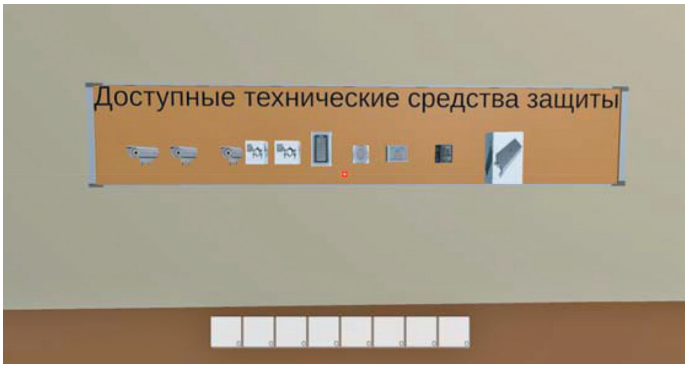

Рис. 2. Интерфейсная часть диалогового окна пространства виртуальной лаборатории «Инженерно-техническая защита информации» с доступным набором средств защиты

Источник: создано М.В. Тумбинской, Б.И. Гатауллиным, Э.И. Хаеровой.

Figure 2. The interface part of the dialog box of the virtual laboratory space *Engineering and Technical Information Protection* with an available set of security tools

Source: created by Marina V. Tumbinskaya, Bulat I. Gataullin, Endzhe I. Haerova.

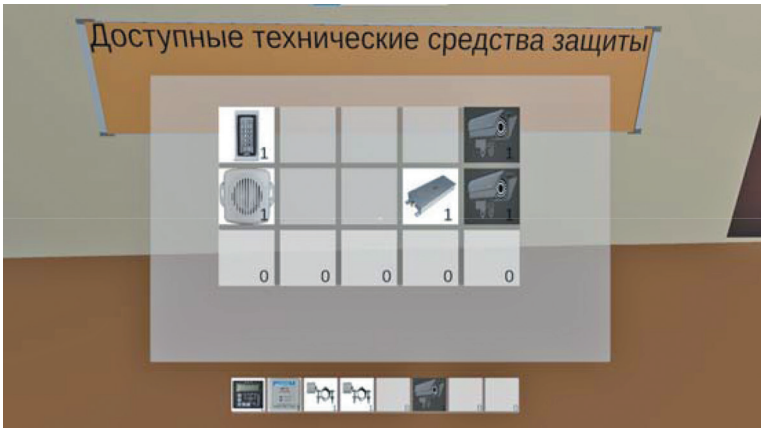

Рис. 3. Интерфейс диалогового окна пространства виртуальной лаборатории «Инженерно-техническая защита информации» выбора и размещения средств защиты

Источник: создано М.В. Тумбинской, Б.И. Гатауллиным, Э.И. Хаеровой.

Figure 3. Interface of the dialog box of the virtual laboratory space *Engineering and Technical Information Protection* for the selection and placement of security tools

Source: created by Marina V. Tumbinskaya, Bulat I. Gataullin, Endzhe I. Haerova.

В процессе изучения раздела «Инженерно-техническая защита информации» была проведена сравнительная оценка качества обучения двух групп студентов. Первая группа выполняла практические задания с использованием виртуальной лаборатории и традиционными методическими указаниями; вторая – только с использованием традиционных методических материалов. Анализ результатов показал, что возможности применения виртуальной лаборатории в учебном процессе позволили повысить качество обучения (табл.).

Результаты второго этапа экспериментального исследования

№ группы	Среднее время размещения одного ТСЗИ	Процент правильного размещения ТСЗИ с первого раза, %	Среднее количество ошибок, ошибка	Среднее время изучение характеристик технических устройств, мин	Среднее время выполнения всей работы, мин
1	44 с	86	2	20	61
2	1 мин 25 с	15	5	30	82

Источник: составлено М.В. Тумбинской, Б.И. Гатауллиным, Э.И. Хаеровой.

Results of the second stage of the experimental study

Group number	Average time of placement of one technical means of information protection	Percent correct placement the first time, %	Average number of errors, error	Average time to study the characteristics of technical devices, min	Average time to complete all work, min
1	44 sec	86	2	20	61
2	1 min 25 sec	15	5	30	82

Source: compiled by Marina V. Tumbinskaya, Bulat I. Gataullin, Endzhe I. Haerova.

Использование виртуальной лаборатории повысило эффективность: сократило время на 23 % (на 21 мин), увеличило точность и снизило ошибки. Студенты проявляли большую самостоятельность и мотивацию.

На третьем этапе исследования проведено тестирование, оценивающее компетенции обучающихся правильно размещать ТСЗИ. Установлено, что 92 % обучающихся группы 1 показали высокий уровень компетенций по сравнению с группой 2 – 52,6 %, что подтверждает эффективность применения лаборатории в формировании профессиональных навыков в области технической защиты информации. Эксперимент показал, что такие средства, как ФЭПС-10, SEL SP-157 (разные модификации), МП-8 «Сигма-РА», СКУД ATIS № 4 и IP-камера ST-183M, не вызывают у обучающихся значительных трудностей при размещении на объекте информатизации (рис. 4). Однако средства с иным принципом действия вызывают сложности на практике.

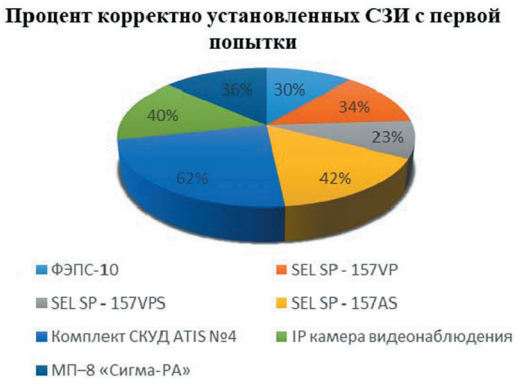

Рис. 4. Диаграмма корректно установленных средств защиты информации с первой попытки

Источник: создано М.В. Тумбинской, Б.И. Гатауллиным, Э.И. Хаеровой.

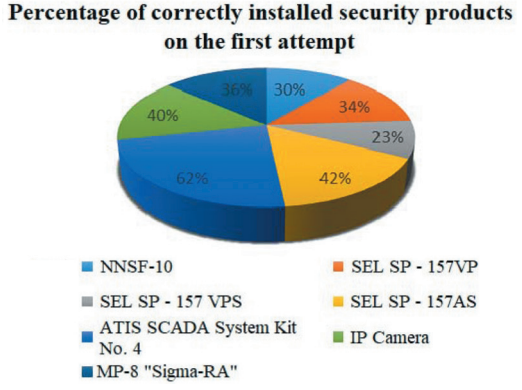

Figure 4. Diagram of correctly installed information security tools on the first attempt

Source: created by Marina V. Tumbinskaya, Bulat I. Gataullin, Endzhe I. Haerova.

Применение виртуальной лаборатории позволило повысить качество обучения за счет увеличения точности решения задач, сокращения временных затрат на выполнение кейсов и снижения частоты ошибок. Возможности применения виртуальной лаборатории в практической подготовке специалистов по ИБ подтверждают целесообразность ее использования для решения реальных задач инженерно-технической ЗИ.

Заключение. Виртуальная инженерно-техническая лаборатория, реализованная на платформе Unity, используется в учебном процессе Казанского национального исследовательского технического университета им. А.Н. Туполева – КАИ и раскрывает возможности практической подготовки специалистов по информационной безопасности за счет имитации решения реальных профессиональных задач в области инженерно-технической ЗИ. Перспективы ее развития связаны с интеграцией технологий виртуальной и дополненной реальности, что позволит формировать иммерсивные учебные среды и обеспечивать более глубокую приближенность образовательного процесса к условиям реальной профессиональной деятельности.

Список литературы

[1] *Григорьева И.В., Поветкин А.С.* Интеграция дополненной реальности (AR) и виртуальной реальности (VR) в образование: тренды, вызовы и перспективы // Вестник Университета Российского инновационного образования. 2025. № 2. С. 38–46. http://doi.org/10.24412/3034-3445-2025-2-38-46 EDN: BEPFHI

[2] *Васенина-Кириллова О.А., Евдокимова В.Е.* Методический инструментарий применения технологии виртуальной реальности в обучении математическим и информационно-технологическим дисциплинам // Современные наукоемкие технологии. 2025. № 9. С. 204–209. http://doi.org/10.17513/snt.40508 EDN: FYBHMW

[3] *Вешнева И.В., Большаков А.А., Асланов Р.Э., Малько Е.И.* Технологии виртуальной и дополненной реальности в образовании: проблемы, перспективы, реализация // Математические методы в технологиях и технике. 2025. № 3. С. 124–134. EDN: HKUPXH

[4] *Москаленко Н.Т., Кардакова М.В., Согонов С.А., Кошанский А.Д.* Образовательная платформа тренажер для специалистов в сфере информационной безопасности // Математические методы в технологиях и технике. 2025. № 1. С. 82–85. EDN: THFUWX

[5] *Ситдикова И.П., Абдулкина Н.В., Дуткин А.С., Рамазанов К.Р.* Виртуальный тренажер на основе высокоточной информационной модели объекта // Известия Тульского государственного университета. Технические науки. 2024. № 12. С. 203–208. http://doi.org/10.24412/2071-6168-2024-12-203-204 EDN: VFRPRA

[6] *Хаерова Э.И., Тумбинская М.В., Гарифуллин Р.Ф.* VR-тренажер по обработке конфиденциальных данных на физическом носителе // Информатизация образования и науки. 2024. № 2(62). С. 62–76. EDN: DYYOKD

[7] *Шпак В.А., Кремлев Е.С., Михайлова У.В.* Разработка виртуального тренажера для оценки защищенности акустической информации в контролируемом помещении // Вестник УрФО. Безопасность в информационной сфере. 2020. № 2(36). С. 10–16. http://doi.org/10.14529/secur200202 EDN: WYVAUA

[8] *Шейхов Г.В., Липатников В.А., Островский Ю.Н., Васильев Н.А., Ледовская К.Г.* Разработка виртуального тренажера по проведению специального обследования объектов информатизации // Региональная информатика и информационная безопасность : сб. трудов Санкт-Петербургской междунар. конф., Санкт-Петербург, 25–27 октября 2023 г. Вып. 12. СПб. : Санкт-Петербургское о-во информатики, вычислительной техники, систем связи и управления, 2023. С. 354–358. EDN: EDQCOP

[9] *Зегжда Д.П.* Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам : монография / Д.П. Зегда, Е.Б. Александрова, М.О. Калинин [и др.]. М. : Горячая линия – Телеком, 2023. 500 с. EDN: BLBTDA

[10] *Осипенко А.А., Чирушкин К.А., Скоробогатов С.Ю., Жданова И.М., Корчевной П.П.* Моделирование компьютерных атак на программно-конфигурируемые сети на основе преобразования стохастических сетей // Известия Тульского государственного университета. Технические науки. 2023. № 2. С. 274–281. http://doi.org/10.24412/2071-6168-2023-2-274-281 EDN: VNGXMX

[11] *Минаев М.В., Бондарь К.М., Дунин В.С.* Моделирование киберустойчивости информационной инфраструктуры МВД России // Криминологический журнал. 2021. № 3. С. 123–128. http://doi.org/10.24412/2687-0185-2021-3-123-128 EDN: EAKMQK

[12] *Бочков М.В., Васинев Д.А.* Метод оценки защищенности критической информационной инфраструктуры // Вопросы кибербезопасности. 2025. № 4(68). С. 17–29. http://doi.org/10.21681/2311-3456-2025-4-17-29 EDN: YXKOLM

[13] *Водопьянов А.С.* Использование цифровых двойников с целью обеспечения информационной безопасности киберфизических систем // Вопросы кибербезопасности.

2024. № 4(62). С. 140–144. http://doi.org/10.21681/2311-3456-2024-4-140-144 EDN: XTJILH

[14] *Жернова К.Н.* Использование интерфейсов виртуальной реальности в области информационной безопасности // Информатизация и связь. 2021. № 2. С. 118–127. http://doi.org/10.34219/2078-8320-2021-12-2-118-127 EDN: WQESIB

References

[1] Grigorieva IV, Povetkin AS. Integration of augmented reality (AR) and virtual reality (VR) in education: trends, challenges and perspectives. *Bulletin of the University of Russian Innovative Education.* 2025;(2):38–46. (In Russ.) http://doi.org/10.24412/3034-3445-2025-2-38-46 EDN: BEPFHI

[2] Vasenina-Kirillova OA, Evdokimova VE. Methodological tools for using virtual reality technology in teaching mathematical and information technology disciplines. *Sovremennye Naukoëmkie Tehnologii = Modern Science-Intensive Technologies.* 2025;(9):204–209. (In Russ.) http://doi.org/10.17513/snt.40508 EDN: FYBHMW

[3] Veshneva IV, Bolshakov AA, Aslanov RE, Malko EI. Technologies of virtual and augmented reality in education: problems, prospects, implementation. *Matematicheskie Metody v Tekhnologiyakh i Tekhnike = Mathematical Methods in Technology and Engineering.* 2025;(3):124–134. (In Russ.) EDN: HKUPXH

[4] Moskalenko NT, Kardakova MV, Sogonov SA, Koshansky AD. Educational platform trainer for information security specialists. *Matematicheskie Metody v Tekhnologiyakh i Tekhnike = Mathematical Methods in Technology and Engineering.* 2025;(1):82–85. (In Russ.) EDN: THFUWX

[5] Sitdikova IP, Abdulkina NV, Dutkin AS, Ramazanov KR. Virtual simulator based on a high-precision information model of the object. *Izvestiya Tula State University. Technical Sciences.* 2024;(12):203–208. (In Russ.) http://doi.org/10.24412/2071-6168-2024-12-203-204 EDN: VFRPRA

[6] Haerova EI, Tumbinskaya MV, Garifullin RF. VR-simulator for processing confidential data on a physical medium. *Informatizatsiya Obrazovaniya i Nauki = Informatization of Education and Science.* 2024;(2):62–76. (In Russ.) EDN: DYYOKD

[7] Shpak VA., Kremlev ES, Mikhailova UV. Development of a virtual trainer for assessing the protection of acoustic information in a controlled room. *Journal of the Ural Federal District. Information Security.* 2020;(2):10–16. (In Russ.) http://doi.org/10.14529/secur200202 EDN: WYVAUA

[8] Sheikhov GV, Lipatnikov VA, Ostrovsky YuN, Vasiliev NA, Ledovskaya KG. Development of a virtual simulator for conducting a special survey of informatization objects. In: *Regional Informatics and Information Security: Proceedings of the St. Petersburg International Conference, October 25–27, 2023, Saint Petersburg.* Saint Petersburg: St. Petersburg Society of informatics, Computer Engineering, Communication Systems and Control Publ.; 2023. issue 12, p. 354–358. (In Russ.) EDN: EDQCOP

[9] Zegzhda DP, Alexandrova EB, Kalinin MO, et al. *Cybersecurity of the Digital Industry. Theory and Practice of Functional Resistance to Cyber Attacks.* Moscow: Goryachaya Liniya – Telekom Publ.; 2023. 500 p. (In Russ.) EDN: BLBTDA

[10] Osipenko AA, Chirushkin KA, Skorobogatov SYu, Zhdanova IM, Korchevnoy PP. Simulation of computer attacks on software-configured networks based on stochastic networks transformation. *Izvestiya Tula State University. Technical Sciences.* 2023;(2):274–281. (In Russ.) http://doi.org/10.24412/2071-6168-2023-2-274-281 EDN: VNGXMX

[11] Minaev MV, Bondar KM, Dunin VS. Modeling of cyber resilience information infrastructure of the internal Affairs Ministry of Russia. *Criminological Journal.*

2021;(3):123–128. (In Russ.) http://doi.org/10.24412/2687-0185-2021-3-123-128 EDN: EAKMQK

[12] Bochkov MV, Vasinev DA. Method assessment of critical information infrastructure security on the basis of semi-natural and simulation modeling tools. *Voprosy Kiberbezopasnosti.* 2025;(4):17–29. (In Russ.) http://doi.org/10.21681/2311-3456-2025-4-17-29 EDN: YXKOLM

[13] Vodopyanov AS. Using digital twins to ensuring information security of cyber physical systems. *Voprosy Kiberbezopasnosti.* 2024;(4):140–144. (In Russ.) http://doi.org/10.21681/2311-3456-2024-4-140-144 EDN: XTJILH

[14] Zhernova KN. The use of virtual reality interfaces in the field of information security. *Informatization and Communications*. 2021;(2):118–127. (In Russ.) http://doi.org/10.34219/2078-8320-2021-12-2-118-127 EDN: WQESIB

Сведения об авторах:

Тумбинская Марина Владимировна, кандидат технических наук, доцент кафедры динамики процессов и управления, Институт компьютерных технологий и защиты информации, Казанский национальный исследовательский технический университет им. А.Н. Туполева – КАИ, Российская Федерация, 420111, Республика Татарстан, Казань, ул. К. Маркса, д. 10. ORCID: 0000-0003-3738-5242; SPIN-код: 4414-9302. E-mail: tumbinskaya@inbox.ru

Гатауллин Булат Ильнурович, студент, специалитет, 5-й курс, Институт компьютерных технологий и защиты информации, Казанский национальный исследовательский технический университет им. А.Н. Туполева – КАИ, Российская Федерация, 420111, Республика Татарстан, Казань, ул. К. Маркса, д. 10. ORCID: 0009-0004-0202-0117; SPIN-код: 6167-4265. E-mail: mr.bulgat12@mail.ru

Хаерова Эндже Ильдаровна, студент магистратуры, Институт компьютерных технологий и защиты информации, Казанский национальный исследовательский технический университет им. А.Н. Туполева – КАИ, Российская Федерация, 420111, Республика Татарстан, Казань, ул. К. Маркса, д. 10. ORCID: 0009-0001-1872-2189; SPIN-код: 2965-7150. E-mail: engikhaer@gmail.com

Bio notes:

Marina V. Tumbinskaya, Candidate of Technical Sciences, Associate Professor at the Department of Process Dynamics and Control, Institute for Computer Technologies and Information Protection, Kazan National Research Technical University named after A.N. Tupolev – KAI, 10 K. Marksa St, Kazan, Republic of Tatarstan, 420111, Russian Federation. ORCID: 0000-0003-3738-5242; SPIN-code: 4414-9302. E-mail: tumbinskaya@inbox.ru

Bulat I. Gataullin, Student, 5th year of specialization, Institute for Computer Technologies and Information Protection, Kazan National Research Technical University named after A.N. Tupolev – KAI, 10 K. Marksa St, Republic of Tatarstan, Kazan, 420111, Russian Federation. ORCID: 0009-0004-0202-0117; SPIN-code: 6167-4265. E-mail: mr.bulgat12@mail.ru

Endzhe I. Haerova, Master's Student, Institute for Computer Technologies and Information Protection, Kazan National Research Technical University named after A.N. Tupolev – KAI, 10 K. Marx St, Kazan, Republic of Tatarstan, 420111, Russian Federation. ORCID: 0009-0001-1872-2189; SPIN-code: 2965-7150. E-mail: engikhaer@gmail.com