

© А.С. Зуфарова

Научная статья
УДК 37.01:007

СИМУЛЯЦИОННАЯ МОДЕЛЬ ОБУЧЕНИЯ: КОНЦЕПЦИЯ, ВИДЫ, ПРЕИМУЩЕСТВА И ПЕРСПЕКТИВЫ

А.С. Зуфарова

Зуфарова Анна Сергеевна,

старший преподаватель кафедры математических методов защиты информации и компьютерной безопасности, Тихоокеанский государственный университет, Хабаровск, Россия.

006694@togudv.ru

Аннотация. *Симуляционная модель обучения представляет собой инновационный подход, позволяющий воссоздавать реальные ситуации и процессы в безопасной учебной среде. В статье рассматривается сущность симуляционного обучения, его классификация по типу среды и предметной области. Особое внимание уделено преимуществам симуляционного подхода: практической направленности, безопасности, индивидуальности, повторяемости и высокой мотивации учащихся. Приводятся примеры успешного применения симуляционных моделей в различных сферах: от хирургических тренажёров в медицине и лётных симуляторов в авиации до киберполигонов для подготовки специалистов по информационной безопасности. Даются основные определения и раскрывается терминологический аппарат в области симуляционного обучения. Центральное место в работе занимает описание педагогического эксперимента, целью которого было сравнение эффективности классической и симуляционной моделей обучения студентов по специальности «информационная безопасность». В рамках исследования было установлено, что студенты, прошедшие подготовку с использованием симуляционных тренировок (фишинговые атаки, отражение DDoS, реагирование на инциденты), продемонстрировали значительно более высокий уровень сформированности практических компетенций. Они успешнее справлялись с распознаванием угроз, созданием надёжных паролей и организацией командной защиты сети. Кроме того, экспериментальная группа проявила большую инициативу, самостоятельность и креативность в решении нестандартных задач. Отдельно выделены перспективы развития симуляционных технологий: внедрение виртуальной и дополненной реальности, искусственный интеллект для генерации реалистичных сценариев, масштабирование через облачные технологии и интеграция в национальные образовательные стандарты. Статья подводит к выводу, что симуляционная модель обучения — это эффективный инструмент подготовки высококвалифицированных специалистов, способный трансформировать образовательный процесс и подготовить новое поколение профессионалов, готовых к реальным вызовам XXI века.*

Ключевые слова: симуляционная модель, обучение, кибербезопасность, методы обучения, симуляция, симуляционные технологии.

Библиографическая ссылка: *Зуфарова А.С. Симуляционная модель обучения: концепция, виды, преимущества и перспективы // ЦИТИСЭ. 2026. № 2. С. 162-172.*

Research Full Article

UDC 37.01:007

SIMULATION MODEL OF LEARNING: CONCEPT, TYPES, ADVANTAGES AND PROSPECTS

A.S. Zufarova

Anna S. Zufarova,

Senior Lecturer at the Department Mathematical
Methods of Information Security and Computer
Security, Pacific State University, Khabarovsk,
Russian Federation.
006694@togudv.ru

Abstract. *The simulation learning model is an innovative approach that allows you to recreate real situations and processes in a safe learning environment. The article examines the essence of simulation learning, its classification by type of environment and subject area. Special attention is paid to the advantages of the simulation approach: practical orientation, safety, individuality, repeatability and high motivation of students. Examples of successful application of simulation models in various fields are given: from surgical simulators in medicine and flight simulators in aviation to cyber training grounds for information security specialists. The basic definitions are given and the terminological apparatus in the field of simulation training is revealed. The central place in the work is occupied by the description of a pedagogical experiment, the purpose of which was to compare the effectiveness of classical and simulation models of teaching students in the specialty "information security". As part of the study, it was found that students who were trained using simulation training (phishing attacks, DDoS reflection, incident response) demonstrated a significantly higher level of practical competencies. They were more successful at recognizing threats, creating strong passwords, and organizing team network protection. In addition, the experimental group showed great initiative, independence and creativity in solving non-standard tasks. The prospects for the development of simulation technologies are highlighted separately: the introduction of virtual and augmented reality, artificial intelligence to generate realistic scenarios, scaling through cloud technologies and integration into national educational standards. The article concludes that the simulation model of education is an effective tool for training highly qualified specialists, capable of transforming the educational process and preparing a new generation of professionals ready for the real challenges of the 21st century.*

Keywords: *simulation model, training, cybersecurity, teaching methods, simulation, simulation technologies.*

For citation: Zufarova, A.S. (2026). Simulation model of learning: concept, types, advantages and prospects. *CITISE*, 2, 162-172. (In Russian).

Введение.

Современный мир стремительно меняется под влиянием технологического прогресса, предъявляющего всё более высокие требования к качеству и эффективности образовательных процессов. Сегодняшняя реальность диктует необходимость подготовки специалистов, способных уверенно действовать в непредсказуемых и часто экстремальных обстоятельствах, принимая быстрые и точные решения. Классические формы обучения, несмотря на свою проверенность временем, нередко оказываются недостаточными для полноценного освоения сложных профессиональных навыков, особенно в тех отраслях, где цена ошибки крайне высока — медицина, авиация, энергетика, промышленность, безопасность и многие другие сферы. Так, медицинские работники учатся проводить операции и оказывать экстренную помощь на высокоточных манекенах, пилоты отрабатывают аварийные сценарии в авиасимуляторах, инженеры тестируют сложные конструкции в виртуальных средах, а менеджеры развивают лидерские компетенции в игровых моделях корпоративных кризисов [1].

Именно в таких условиях возникла и получила мощное развитие симуляционная модель обучения — революционный подход, позволяющий воссоздавать реальные профессиональные ситуации в контролируемой и безопасной среде. Эта методика зародилась в середине XX века, первоначально получив широкое распространение в авиации, где важность безупречного владения техникой пилотирования была вопросом жизни и смерти [2]. Постепенно сфера применения симуляционного обучения расширялась, охватывая всё большее количество отраслей, становясь неотъемлемым элементом подготовки специалистов самого различного профиля.

Сегодня симуляционное обучение воспринимается не просто как дополнительный инструмент, а как полноценная альтернатива традиционным методам передачи знаний и навыков. Его популярность обусловлена способностью максимально приближенно моделировать рабочие процессы, позволяя участникам приобретать практический опыт без риска нанести ущерб здоровью людей, имуществу или окружающей среде. Благодаря этому подходу студенты и специалисты получают уникальную возможность многократно повторять упражнения, экспериментировать с различными стратегиями и тактиками, совершать ошибки и учиться на них в комфортной и поддерживающей атмосфере.

Постоянное развитие технологий, таких как виртуальная и дополненная реальность, искусственный интеллект и облачные вычисления, выводит симуляционное обучение на качественно новый уровень. Теперь участники могут взаимодействовать с моделями, максимально близкими к действительности, получать мгновенную обратную связь и детально анализировать собственную работу, выявляя зоны роста и улучшая качество исполнения.

Всё это делает симуляционную модель обучения не просто актуальным направлением, а стратегической необходимостью для любого современного образовательного учреждения и предприятия, заинтересованного в подготовке высококлассных специалистов, готовых эффективно решать задачи завтрашнего дня.

Симуляционная модель обучения стала важным инструментом в современной педагогике, позволяя студентам и профессионалам развивать необходимые навыки в безопасной и контролируемой среде. Данная модель находит своё применение в самых разных областях — от медицины и инженерных наук до гуманитарных дисциплин и бизнеса [3]. За последние годы появилось множество исследований, посвящённых эффективности и особенностям симуляционного обучения, а также разработаны инновационные технологии, такие как виртуальная и дополненная реальность (VR/AR), которые значительно расширили границы возможного в образовательной сфере [16].

Основная часть.

Симуляционные технологии — это система интерактивных методов и подходов, предназначенных для моделирования образовательного процесса. Они предполагают поэтапное конструирование, имитацию и воспроизведение клинических ситуаций с использованием биологических, механических, электронных и виртуальных моделей [4].

Применение симуляционных технологий позволяет студентам развивать такие важные компетенции, как командная работа, партнёрское взаимодействие с коллегами, а также навыки эффективного профессионального и межличичного общения.

Продуктивными формами симуляционного обучения являются [5]:

- Симуляционный тренинг: интенсивная практика в условиях, приближённых к реальным.
- Ролевая игра: моделирование профессиональных ситуаций с распределением ролей.
- Ситуационный анализ (case-study, дебрифинг): разбор конкретных клинических случаев с последующим обсуждением и рефлексией.

Симуляционная модель обучения — это современная образовательная стратегия, направленная на приобретение профессиональных навыков путём погружения обучающихся в искусственно созданные ситуации, максимально близкие к реальным жизненным обстоятельствам [4]. Такой подход обеспечивает безопасную среду для тренировки практических умений, минимизирует последствия возможных ошибок и способствует выработке уверенности и компетентности. Симуляционная модель обучения определяется как техника, позволяющая заместить или обогатить практический опыт обучающегося с помощью искусственно созданной ситуации, которая отражает и воспроизводит проблемы, характерные для реального мира, в полностью интерактивной манере. Она предоставляет возможность каждому учащемуся выполнить профессиональную деятельность или её элемент в соответствии с установленными стандартами и правилами.

Существует несколько разновидностей симуляционных моделей, каждая из которых применяется в зависимости от целей обучения и специфики профессии [2; 3;10]:

1. Физические симуляторы (манекены, тренажёры). Используются для отработки физических навыков, например, в медицине (сердечно-лёгочная реанимация, хирургические манипуляции) или пилотировании самолётов.
2. Компьютерные симуляции. Моделируют сложные процессы и системы, позволяя исследовать поведение объектов и явлений в контролируемых условиях (экономические модели, экологические катастрофы).
3. Виртуальная реальность (VR). Полностью погружает пользователя в смоделированную обстановку, обеспечивая реалистичное взаимодействие с объектами и средой.
4. Дополненная реальность (AR). Объединяет реальную и виртуальную среду, накладывая цифровые объекты на физическое окружение.
5. Ролевые игры и игровые симуляции. Применяются для отработки коммуникативных и управленческих навыков, разрешения конфликтных ситуаций и принятия решений в команде.

В современную цифровую эпоху, когда информационные технологии пронизывают все сферы жизнедеятельности общества, вопросы информационной безопасности приобретают стратегическое значение. Рост числа киберпреступлений, хакерских атак, утечек данных и других угроз ставит перед специалистами по защите информации новые вызовы, требующие не только глубоких теоретических знаний, но и уверенных практических навыков.

В современном образовательном процессе всё большее значение приобретает практическая составляющая обучения, особенно в таких динамично развивающихся областях, как кибербезопасность [11]. Классические лекции и семинары, безусловно,

формируют фундаментальные знания, однако для овладения профессией специалиста по защите информации необходим практический опыт, умение быстро принимать решения в стрессовых ситуациях и владеть современными инструментами защиты.

Симуляционные модели обучения позволяют воссоздать реальные сценарии атак, взломов и инцидентов, предоставляя студентам уникальную возможность погрузиться в рабочую обстановку и отработать навыки защиты информации в безопасной учебной среде. Настоящий эксперимент направлен на проверку эффективности симуляционного подхода в обучении студентов кибербезопасности [14].

Классические методы обучения, основанные преимущественно на лекциях и теоретических занятиях, зачастую недостаточны для полноценного освоения профессии эксперта по кибербезопасности. Практический опыт, умение быстро принимать решения в стрессовых ситуациях, владение современными инструментами защиты — всё это достигается лишь через непосредственное погружение в реальные или максимально приближенные к реальности условия [10]. Именно в таком контексте симуляционные модели обучения становятся важнейшим инструментом подготовки специалистов в области кибербезопасности.

Симуляционная модель представляет собой высокотехнологичную среду, воссоздающую реальные сценарии атак, взломов, инцидентов и реагирования на угрозы [7]. Она позволяет ученикам и профессионалам проходить через последовательность практических упражнений, имитирующих реальные угрозы, и приобретать навыки, необходимые для эффективной защиты информационных систем.

Теоретическое основание исследования представлено широким спектром научных концепций и авторов, охватывающих педагогику, компетентностный подход, организацию образования, командообразование, активные методы обучения и симуляционные технологии. Наше исследование базируется на следующих научных направлениях и работах ведущих учёных [1-6]:

1. Педагогика профессионального образования и методология педагогических исследований: работы С.И. Архангельского, С.А. Бешенкова, В.И. Загвязинского, Э.Ф. Зеера, В.А. Сластенина и других авторов, исследовавших вопросы профессионального образования и методологических подходов в педагогике.

2. Компетентностный подход в профессиональном образовании: идеи В.И. Байденко, В.А. Болотова, И.А. Зимней, А.М. Новикова, А.В. Хуторского и других исследователей, развивавших концепцию формирования профессиональных компетенций.

3. Командно-ориентированное обучение: исследования С.Б. Ахметовой, Н.П. Клушиной, L. Michaelsen, M. Sweet и других авторов, изучавших вопросы командной работы и коллаборативного обучения.

4. Активные и интерактивные методы обучения: работы В.Я. Вульфберта, Е.В. Зарукиной, Е.С. Полат и других учёных, развивавших интерактивные подходы в медицинском образовании.

5. Симуляционное обучение в образовании: исследования А.Н. Архипова, П.В. Глыбочко, М.П. Гринберга и других авторов, изучавших организацию симуляционных технологий в подготовке специалистов.

6. Формирование профессиональных компетенций с помощью симуляционных технологий: работы С.А. Батова, Е.В. Волчковой, Ю.В. Королёвой, J.W. Crommett и других исследователей, изучавших влияние симуляционных методов на подготовку медицинских специалистов.

Такой комплексный подход позволяет всесторонне исследовать феномен симуляционного обучения и его вклад в подготовку высококвалифицированных специалистов в области кибербезопасности.

Симуляционные технологии — система интерактивных методов и способов моделирования образовательного процесса, основанная на поэтапном конструировании, имитации и воспроизведении ситуаций с применением механических, электронных и виртуальных моделей [8].

Симуляционные технологии обеспечивают формирование у студентов компетенцию командной работы, партнерского взаимодействия с коллегами, а также навыки и умения эффективного профессионального и межличностного общения. Продуктивными формами симуляционного обучения выступают симуляционный тренинг, ролевая игра, ситуационный анализ (case-study, дебрифинг) [5].

Научная новизна симуляционного подхода заключается в сочетании теоретических знаний с практическим опытом, развитии критического мышления, стрессоустойчивости и командной работы. Подобная модель обучения позволяет не только освоить инструменты защиты, но и научиться мыслить, как злоумышленник, предугадывать его действия и выстраивать стратегию защиты.

Актуальность исследования симуляционных моделей обусловлена стремительным развитием цифровых угроз, необходимостью подготовки высококвалифицированных кадров и постоянным спросом на специалистов, способных оперативно реагировать на новые вызовы информационной безопасности.

Цель данного исследования — изучить эффективность симуляционных моделей обучения в подготовке специалистов по кибербезопасности, выявить их преимущества и ограничения, а также предложить рекомендации по совершенствованию образовательных программ на основе симуляционного подхода.

В дальнейшем исследовании планируется рассмотреть конкретные примеры симуляционных сред, проанализировать их влияние на профессиональные компетенции обучающихся, а также предложить методологию внедрения симуляционных моделей в учебный процесс образовательных учреждений и корпоративных тренинг-центров.

Рассмотрим эксперимент по внедрению симуляционной модели обучения в кибербезопасности.

Методология эксперимента.

В нашем эксперименте участвовало две группы студентов обучающей по профильной специальности в области информационной безопасности с 01.09.2025 по 31.12.2025. За это период обучения студенты проходили программу по защите информации и студенты были распределены на две группы.

«Группа А» (классическая форма обучения): 15 студентов, обучавшихся по классической программе (лекции, семинары, лабораторные и практические работы).

«Группа В» (экспериментальная форма обучения): 15 студентов, прошедших дополнительное обучение по симуляционной модели в области кибербезопасности.

Обе группы студентов проходили стандартный курс по кибербезопасности: слушали лекции, выполняли практические и лабораторные работы, работали на семинарах и выполняли курсовые работы. Но экспериментальная «группа В» в добавок участвовала в еженедельных симуляционных тренировках в области кибербезопасности.

Им были предоставлены следующие симуляционные тренировки в рамках изучения дисциплины [15, 9].

1. Симуляция фишинговой атаки. Студенты получали поддельные письма, имитирующие различные уведомления от различных учреждений. Письма содержали фишинговые ссылки, вложения, QR коды. Их задача состояла, распознать фишинговые письма и не попасть на уловку мошенника [12].

2. Симуляция взлома пароля. Студенты создавали пароли различной сложности. Затем симулятор-программа пытался их взломать. Задача, стоящая перед обучающимися, научиться создавать стойкие пароли по выбранным алгоритму.

3. Симуляция DDoS-атаки. Студенты управляли виртуальной сетью, на которую поступала волна запросов. Задача обучающихся настроить надежную защиту и успешно отразить атаку.

4. Симуляция утечки данных: Студенты обнаруживали инцидент (утечка базы клиентов). Задача, стоящая перед ними, провести расследование, локализовать причину и устранить последствия.

5. Командная защита сети. Группа защищала виртуальную сеть от атак, проводимых преподавателем в полигоне. Задача учащихся, скоординировать свои усилия, выбрать правильную тактику обороны и распределить обязанности в группе.

6. Интерактивная форма в виде квеста «Красный код». Команда анализировала и расследовала инциденты. Восстанавливала систему после взлома. Задача учащихся с помощью основ цифровой криминалистики собрать улики, найти злоумышленника, восстановить данные.

Наша гипотеза эксперимента состоит в том, что студенты, прошедшие по симуляционной модели обучения, покажут более высокий уровень компетенций в области кибербезопасности по сравнению с группой, обучавшейся по классической схеме обучения. Ниже представлены наши результаты исследования по истечению срока обучения.

На первом этапе было проведено тестирование теоретических знаний: «Группа А»: получен средний балл — $78 \% \pm 5$ и «Группа В» получен средний балл — $82\% \pm 4$. Различие незначительное, что свидетельствует о равнозначном усвоении теоретического материала.

На втором этапе было проведено практическое тестирование навыков.

Задача 1: Распознавание фишинговых писем. Контрольная «Группа А»: 65% правильных ответов. Экспериментальная «Группа В»: 89% правильных ответов.

Задача 2: Создание надёжных паролей. Контрольная «Группа А»: 40% создали надёжные пароли. Экспериментальная «Группа В»: 85% создали надёжные пароли.

Задача 3: Защита сети от DDoS-атаки. Контрольная «Группа А»: 30% смогли отразить атаку. Экспериментальная «Группа В»: 75% успешно защитили сеть.

Задача 4: Инцидентное реагирование (утечка данных). Контрольная «Группа А»: 20% решили задачу полностью. Экспериментальная «Группа В»: 65% решили задачу полностью.

На третьем этапе была проведена анкетирование участников эксперимента [7].

Были заданы интересующие вопросы для нашего исследования. Первый один из них «Насколько вы чувствуете себя готовым к работе в сфере кибербезопасности?» Контрольная «Группа А»: средняя оценка — 6,5 из 10. Экспериментальная «Группа В»: средняя оценка — 8,7 из 10. Второй вопрос: «Какой метод обучения был наиболее полезным?». Контрольная «Группа А»: 45% назвали лекции, 38% — лабораторные работы. Экспериментальная «Группа В»: 85% назвали симуляционные тренировки.

Можно подметить, что студенты экспериментальной «Группа В» проявляли большую инициативу и самостоятельность; лучше работали в команде, и распределяя обязанности; продемонстрировали креативный подход к решению задач.

Обсуждение результатов.

Эксперимент показал, что симуляционная модель обучения значительно повышает уровень практических навыков студентов в области кибербезопасности. Студенты, прошедшие симуляционные тренировки, показали: более высокий уровень распознавания фишинговых атак (+24%), гораздо лучшее умение создавать надёжные пароли (+45%), значительно возросшую способность отражать атаки и реагировать на инциденты (+45% и +45%).

Помимо количественных показателей, качественные наблюдения также подтвердили эффективность симуляционного подхода. Студенты экспериментальной группы продемонстрировали: большую уверенность в своих силах, лучшую готовность к работе в реальных условиях, более высокий уровень командной работы и творческого мышления [9].

Заключение.

Результаты эксперимента однозначно подтверждают выдвинутую гипотезу: симуляционная модель обучения значительно превосходит классический подход в формировании профессиональных компетенций в области кибербезопасности. Студенты, прошедшие обучение с использованием симуляторов, показали более высокий уровень практических навыков, уверенности и готовности к профессиональной деятельности.

На основании полученных данных можно рекомендовать внедрение симуляционных тренировок в образовательные программы вузов, колледжей и корпоративных тренингов. Такой подход позволит готовить квалифицированных специалистов, готовых эффективно противостоять современным киберугрозам.

Практические рекомендации:

1. Внедрить симуляционные тренировки в учебные планы вузов, колледжей.
2. Разработать стандарты сертификации для симуляционных центров.
3. Создавать библиотеки сценариев атак для регулярного обновления учебных программ.
4. Проводить ежегодные соревнования по кибербезопасности с использованием симуляционных платформ.

Нами экспериментально доказано, что симуляционная модель обучения значительно превосходит классические методы в формировании практических навыков специалистов по кибербезопасности. Полученные результаты могут служить основой для разработки новых образовательных стандартов и программ в области защиты информации.

Перспективы дальнейших исследований могут быть направлены на различные направления:

1. Развитие искусственного интеллекта для генерации реалистичных сценариев атак, например фишинговых.

Фишинг по-прежнему остаётся одним из наиболее часто используемых и опасных способов кибератак, при этом стандартные методы обучения пользователей не всегда дают желаемый результат. Решить эту проблему помогает применение искусственного интеллекта для создания индивидуальных учебных материалов. Такой подход позволяет учитывать личные особенности каждого обучающегося — его уровень подготовки, предпочтения в способах восприятия информации и интересы, что делает образовательный процесс гораздо более результативным.

2. Изучение влияния симуляционных тренировок на профессиональное выгорание специалистов.

Профессиональное выгорание — это состояние эмоционального, физического и умственного истощения, возникающее вследствие длительного стресса на работе. Особенно подвержены выгоранию специалисты, работающие в условиях высокой ответственности и постоянного напряжения (врачи, педагоги, спасатели, сотрудники экстренных служб). Симуляционные тренировки — это метод обучения, при котором воссоздаются реалистичные рабочие ситуации для отработки навыков и принятия решений в безопасной среде. Они позволяют специалистам безопасно приобретать опыт, развивать стрессоустойчивость и уверенность в своих силах, что в итоге способствует сохранению психоэмоционального здоровья и повышению качества профессиональной деятельности.

3. Внедрение геймификации в симуляционные модели для повышения мотивации обучающихся.

Геймификация — это использование игровых элементов (баллы, достижения, рейтинги, сюжетные линии) в неигровых процессах для повышения вовлечённости и мотивации. Внедрение геймификации в симуляционные модели — эффективный способ повысить мотивацию обучающихся, сделать процесс обучения более увлекательным и

результативным. Такой подход способствует не только освоению профессиональных навыков, но и формированию позитивного отношения к обучению в целом.

Симуляционная модель обучения — это прорывной подход в подготовке специалистов по кибербезопасности. Экспериментальные данные подтверждают её эффективность и открывают новые горизонты для совершенствования образовательных программ в области защиты информации.

Список источников:

1. Абдумуталова М.М. Симуляционное обучение в медицине: проблемы, решения, перспективы // Вестник науки. 2023. Т. 5, № 10(67). С. 739-745. URL: <https://www.elibrary.ru/plwzcb>
2. Бондаренко Е.В., Хоронько Ю.В. Симуляционное обучение как ведущее направление развития медицины // Мир науки. Педагогика и психология. 2022. Т. 10, № 3. URL: <https://www.elibrary.ru/dnsmvi>
3. Антипова И.Н., Карибян К.В., Свиридова Т.Б., Комарова Е.А. Значение симуляционных технологий в практическом обучении медицинских работников в России // Научный аспект. 2024. Т. 16, № 3. С. 1885-1895. URL: <https://www.elibrary.ru/acfafi>
4. Мирзахмедова Ш.А. Симуляционное обучение в профессиональном образовании // Проблемы современной науки и образования. 2021. № 4(161). С. 61-63. URL: <https://www.elibrary.ru/acfafi>
5. Чечик Н.М., Абельская И.С. Анализ эффективности обучения с использованием симуляционных технологий // Виртуальные технологии в медицине. 2023. № 3(37). С. 215-217. DOI: https://doi.org/10.46594/2687-0037_2023_3_1690
6. Хусаинова Г.С., Ткачев В.А., Сулейменова Ш.Б., Омиртаева Б.А. Применение симуляционного обучения в учебном процессе // Биология и интегративная медицина. 2021. № 6(53). С. 420-423. URL: <https://www.elibrary.ru/tiolup>
7. Жданова Д.Е. Технология реверсивного обучения: сочетание мобильного обучения и активных методов обучения // Наукосфера. 2021. № 7-1. С. 55-58. URL: <https://www.elibrary.ru/siqyud>
8. Нечипуровский Д.И. Как построить многоуровневую защиту для борьбы с продвинутыми угрозами фишинга // Научный аспект. 2024. Т. 41, № 4. С. 5337-5342. URL: <https://www.elibrary.ru/jdtfvy>
9. Яковлева М.А. Лидерство в системе наставничества как эффективный инструмент адаптации персонала // Human Progress. 2021. Т. 7, № 1. DOI: <https://doi.org/10.34709/IM.171.17>
10. Сапармаммедова Г. Интеграция цифровых технологий в симуляционное обучение // Инновационная наука. 2025. № 5-2. С. 231-232. URL: <https://www.elibrary.ru/ndcisq>
11. Дорофеев А.В., Марков А.С. Применение отечественных технологий для мониторинга информационной безопасности в условиях импортозамещения // Защита информации. Инсайд. 2023. № 3(111). С. 20-26. URL: <https://www.elibrary.ru/fdptdw>
12. Ан Д.С., Зуфарова А.С. Симуляция фишинговых атак как метод повышения киберграмотности и подготовки к реагированию на угрозы // Управление образованием: теория и практика. 2025. № 6-1. С. 127-139. DOI: <https://doi.org/10.25726/b2476-6563-8129-i>
13. Лопатин Д.В., Анурьева М.С. Разработка ситуационных тренажеров как элемент подготовки специалистов по защите информации // Образование и право. 2022. № 10. С. 121-127. DOI: <https://doi.org/10.24412/2076-1503-2022-10-121-127>
14. Акапьев В.Л., Дунаев Е.Г. К вопросу о разработке виртуального симулятора киберугроз // Bulletin of Art and Education. 2025. № 7. С. 289-300. URL: <https://www.elibrary.ru/qiozat>

15. Атаманов Б.Я., Чуриев М.М., Гельдыева М.А., Чарыева Д.Д. Разработка и применение симулятора активной кибератаки // Математические методы в технологиях и технике. 2023. № 12. С. 105-111. DOI: https://doi.org/10.52348/2712-8873_MMTT_2023_12_105
16. Шайхулов Э.А., Смирнов А.П., Болдина О.Б. Современные методы обучения информационной безопасности // Современная наука и инновации. 2023. № 4(44). С. 145-151. DOI: <https://doi.org/10.37493/2307-910X.2023.4.16>

References:

1. Abdumutalova, M. M. (2023). Simulation training in medicine: Problems, solutions, prospects. *Bulletin of Science*, 5(10), 739–745. (In Russian). <https://www.elibrary.ru/plwzcb>
2. Bondarenko, E. V., & Khoronko, Yu. V. (2022). Simulation training as a leading direction in the development of medicine. *The World of Science. Pedagogy and Psychology*, 10(3). (In Russian). <https://www.elibrary.ru/dnsmvi>
3. Antipova, I. N., Karibyan, K. V., Sviridova, T. B., & Komarova, E. A. (2024). The importance of simulation technologies in the practical training of medical workers in Russia. *Scientific Aspect*, 16(3), 1885–1895. (In Russian). <https://www.elibrary.ru/acfafi>
4. Mirzakhmedova, Sh. A. (2021). Simulation training in vocational education. *Problems of Modern Science and Education*, 4, 61–63. (In Russian). <https://www.elibrary.ru/acfafi>
5. Chechik, N. M., & Abelskaya, I. S. (2023). Analysis of the effectiveness of training using simulation technologies. *Virtual Technologies in Medicine*, 3, 215–217. (In Russian). https://doi.org/10.46594/2687-0037_2023_3_1690
6. Khusainova, G. S., Tkachev, V. A., Suleimenova, Sh. B., & Omirtaeva, B. A. (2021). Application of simulation learning in the educational process. *Biology and Integrative Medicine*, 6, 420–423. (In Russian). <https://www.elibrary.ru/tiolup>
7. Zhdanova, D. E. (2021). Reverse learning technology: A combination of mobile learning and active learning methods. *Naukosfera*, 7–1, 55–58. (In Russian). <https://www.elibrary.ru/siqyud>
8. Nechipurovsky, D. I. (2024). How to build a multi-layered defense to combat advanced phishing threats. *Scientific Aspect*, 41(4), 5337–5342. (In Russian). <https://www.elibrary.ru/jdtfvy>
9. Yakovleva, M. A. (2021). Leadership in the mentoring system as an effective tool for personnel adaptation. *Human Progress*, 7(1). (In Russian). <https://doi.org/10.34709/IM.171.17>
10. Saparmammedova, G. (2025). Integration of digital technologies into simulation training. *Innovative Science*, 5–2, 231–232. (In Russian). <https://www.elibrary.ru/ndcisq>
11. Dorofeev, A. V., & Markov, A. S. (2023). Application of domestic technologies for monitoring information security in the context of import substitution. *Information Protection. Inside*, 3, 20–26. (In Russian). <https://www.elibrary.ru/fdptdw>
12. An, D. S., & Zufarova, A. S. (2025). Simulation of phishing attacks as a method of improving cyber literacy and preparing to response to threats. *Education Management: Theory and Practice*, 6–1, 127–139. (In Russian). <https://doi.org/10.25726/b2476-6563-8129-i>
13. Lopatin, D. V., & Anureva, M. S. (2022). Development of situational simulators as an element of training information security specialists. *Education and Law*, 10, 121–127. (In Russian). <https://doi.org/10.24412/2076-1503-2022-10-121-127>
14. Akayev, V. L., & Dunaev, E. G. (2025). On the development of a virtual cyber threat simulator. *Bulletin of Art and Education*, 7, 289–300. (In Russian). <https://www.elibrary.ru/qiozat>
15. Atamanov, B. Ya., Churiev, M. M., Geldyeva, M. A., & Charyeva, D. D. (2023). Development and application of an active cyber attack simulator. *Mathematical Methods in Technology and Engineering*, 12, 105–111. (In Russian). https://doi.org/10.52348/2712-8873_MMTT_2023_12_105

16. Shaikhulov, E. A., Smirnov, A. P., & Boldina, O. B. (2023). Modern methods of teaching information security. *Modern Science and Innovation*, 4, 145–151. (In Russian). <https://doi.org/10.37493/2307-910X.2023.4.16>

Submitted: 25 March 2026

Accepted: 26 April 2026

Published: 26 April 2026

