ЦИФРОВИЗАЦИЯ

УДК 37-042.4:004+004.49
DOI 10.20339/AM.02-25.060

Г.Г. Егоров,
канд. юр. наук, доцент, научный сотрудник
Волжский филиал Волгоградского государственного университета, г. Волжский
https://orcid.org/0000-0002-5969-1171
Scopus AuthorID: 57208147511
ResearcherID: H-3519-2017
GoogleScholarID: hOml0CsAAAAJ
SPIN-код: 6194-7154
email: egoov@vgi.volsu.ru

ПЕРСПЕКТИВЫ ИСПОЛЬЗОВАНИЯ СИСТЕМ ВИРТУАЛЬНОГО ОБУЧЕНИЯ В СОВРЕМЕННОМ ОБРАЗОВАНИИ

В данной статье представлен глубокий анализ процесса создания виртуальной образовательной среды (ВОС), которая активно использует инновационный инструмент — программируемый имитатор компьютерных атак. Этот инструмент играет ключевую роль в подготовке специалистов по информационной безопасности. Имитатор позволяет создавать реалистичные сценарии различных видов кибератак, с которыми будущие специалисты могут столкнуться в своей профессиональной деятельности. Благодаря этому студенты получают уникальную возможность отточить свои навыки в области защиты информационных систем в условиях, максимально приближенных к реальным. Подробно рассматриваются особенности построения такой образовательной среды, а также преимущества использования имитатора в учебном процессе. ВОС в области информационной безопасности представляет собой инновационную платформу, которая кардинально меняет традиционные подходы к обучению. Благодаря интерактивному формату обучающиеся имеют возможность активно участвовать в процессе познания, самостоятельно проходя через нелинейные сценарии обучения. Это не только повышает мотивацию, но и способствует более глубокому усвоению материала. Кроме того, активное вовлечение педагога в учебный процесс позволяет обеспечить индивидуальный подход к каждому студенту и оперативно реагировать на возникающие вопросы. Широкое использование информационных технологий делает обучение более динамичным и наглядным. Особое место в этой среде занимают цифровые имитаторы, которые позволяют моделировать реальные кибератаки и оценивать устойчивость компьютерных сетей. Благодаря этому студенты приобретают практические навыки по обнаружению и устранению уязвимостей, что является крайне важным для подготовки высококвалифицированных специалистов в области информационной безопасности. Для создания и развития подобных образовательных сред целесообразно привлекать ведущих производителей программного обеспечения в качестве стратегических партнеров. Такое сотрудничество позволит обеспечить доступ к самым современным технологиям и разработкам, а также создать единое образовательное пространство, отвечающее самым высоким стандартам.

Ключевые слова: *виртуальная образовательная среда (ВОС), программируемый имитатор компьютерных атак, образовательный процесс, информационная безопасность, цифровые системы безопасности.*

PROSPECTS FOR THE USE OF VIRTUAL LEARNING SYSTEMS IN MODERN EDUCATION

Gennady G. Egorov, PhD in Law, Docent, Research Fellow at the Volga Branch of the Volgograd State University, Volzhsky, Volgograd Oblast, https://orcid.org/0000-0002-5969-1171, ScopusAuthorID: 57208147511, ResearcherID: H-3519-2017, GoogleScholarID: hOml0CsAAAAJ, SPIN-code: 6194-7154, email: *egoov@vgi.volsu.ru*

This article presents an in-depth analysis of the process of creating a virtual educational environment (VEE) that actively uses an innovative tool — a programmable simulator of computer attacks. This tool plays a key role in the training of information security specialists. The simulator allows you to create realistic scenarios of various types of cyberattacks that future specialists may encounter in their professional activities. Thanks to this, students get a unique opportunity to hone their skills in the field of information system protection in conditions as close to real as possible. The features of building such an educational environment, as well as the advantages of using the simulator in the educational process, are considered in detail. VEE in the field of information security is an innovative platform that radically changes traditional approaches to learning. Thanks to the interactive format, students have the opportunity to actively participate in the learning process, independently going through non-linear learning scenarios. This not only increases motivation, but also contributes to a deeper assimilation of the material. In addition, the active involvement of the teacher in the educational process allows for an individual approach to each student and a prompt response to emerging issues. The widespread use of information technology makes learning more dynamic and visual. A special place in this environment is occupied by digital simulators, which allow modeling real cyber attacks and assessing the stability of computer networks. Thanks to this, students acquire practical skills in detecting and eliminating vulnerabilities, which is extremely important for training highly qualified specialists in the field of information security. To create and develop such educational environments, it is advisable to attract leading software manufacturers as strategic partners. Such cooperation will provide access to the most modern technologies and developments, as well as create a single educational space that meets the highest standards.

Keywords: *virtual educational environment (VEE), programmable simulator of computer attacks, educational process, information security, digital security systems*

Введение

Современная информационная среда, пронизывающая все сферы нашей жизни, требует от каждого пользователя не только базовых навыков работы с компьютерами и сетями, но и глубокого понимания принципов информационной безопасности [3]. К сожалению, осознание важности защиты персональных данных и конфиденциальности информации пока еще недостаточно распространено среди пользователей. Многие из нас не обладают необходимыми знаниями для того, чтобы эффективно противостоять многочисленным угрозам, которые таит в себе цифровой мир. Именно поэтому специалисты в области информационной безопасности играют ключевую роль в обеспечении нашей защиты. Они должны обладать не только теоретическими знаниями, но и практическими навыками работы с реальными уязвимостями, позволяющими им оперативно выявлять и устранять возникающие угрозы [2]. Данный подход гарантирует надежную защиту информационных систем и данных, что является неотъемлемым условием успешного функционирования современного общества.

Одним из наиболее эффективных инструментов, предоставляющих уникальную возможность получить практический опыт в области информационной безопасности, является программируемый имитатор компьютерных атак. Этот инновационный инструмент позволяет воссоздать в виртуальной среде (ВС) максимально реалистичные условия, имитируя различные типы кибератак, с которыми специалисты могут столкнуться в реальной жизни[1]. Погружаясь в данную ВС, будущие защитники информационных систем получают возможность детально изучить процессы проникновения злоумышленников в систему, выявить уязвимости и отработать алгоритмы действий по их устранению [7]. Благодаря использованию имитатора специалисты могут на практике освоить широкий спектр инструментов и методик, применяемых как хакерами, так и специалистами по информационной безопасности. Это позволяет не только значительно повысить уровень подготовки специалистов, но и минимизировать риски, связанные с проведением реальных атак на производственные системы.

ВОС представляет собой инновационный подход к обучению, который радикально отличается от традиционных методов. Она создает условия, максимально приближенные к реальным жизненным ситуациям, погружая обучающегося в интерактивную среду, где он становится активным участником образовательного процесса. В отличие от пассивного восприятия информации, характерного для традиционных лекций, виртуальная среда стимулирует самостоятельное мышление, принятие решений и развитие практических навыков. Динамический и нелинейный характер обучения позволяет каждому обучающемуся строить свой индивидуальный образовательный маршрут, выбирая наиболее

[1] Платформы симуляции кибератак (Breach and Attack Simulation, BAS) позволяют компаниям постоянно и последовательно моделировать полный цикл атак на ИТ-инфраструктуру. Согласно исследованию Automated Breach and Attack Simulation (BAS) Market Size And Forecast рынок BAS оценивался в 130,82 млн долларов США в 2019 г. и по прогнозам достигнет 1572,59 млн долларов США к 2027 г., увеличиваясь в среднем на 36,47% с 2020 по 2027 г. URL: https://www.anti-malware.ru/analytics/Market_Analysis/Breach-and-Attack-Simulation-Market-Overview (03.02.2025). — *Примеч. ред.*

интересные и актуальные для него темы, при этом не только повышая мотивацию к обучению, но и способствуя развитию творческого потенциала и возможности адаптироваться к быстро меняющимся условиям современного мира.

Реализация эффективного обучения в области цифровой безопасности сопряжена с целым рядом сложностей, которые необходимо учитывать при разработке учебных программ и методик. Одна из главных трудностей заключается в сложности самого программного обеспечения, используемого для обучения. Специализированные инструменты и платформы, предназначенные для моделирования кибератак и защиты от них, часто обладают сложным интерфейсом и требуют глубоких технических знаний. Это может значительно затруднить процесс обучения, особенно для начинающих специалистов [4]. Кроме того, разработка реалистичных и интересных сценариев занятий представляет собой непростую задачу. Слишком упрощенные сценарии не позволяют обучающимся получить глубокие знания и навыки, а слишком сложные могут вызвать у них чувство перегрузки и демотивации. При этом следует учитывать, что предметная область информационной безопасности характеризуется высокой динамичностью. Постоянно появляются новые угрозы, уязвимости и методы защиты, что требует постоянного обновления учебных материалов и адаптации к меняющимся условиям. Создание эффективной системы обучения в области кибербезопасности является комплексной задачей, требующей тщательного анализа и учета всех факторов, влияющих на процесс обучения.

Процесс обеспечения информационной безопасности на сложных объектах часто сравнивают с искусством. Ведь здесь требуется не только знание технических аспектов, но и умение анализировать ситуацию, принимать нестандартные решения и предвидеть возможные угрозы. Современные технологии, в частности, цифровое обучение, позволяют значительно приблизить процесс подготовки специалистов по информационной безопасности к реальным условиям работы [2]. ВОС, основанная на принципах интерактивности и нелинейности, создает уникальные возможности для погружения обучающихся в динамическую среду, имитирующую реальные кибератаки. Она позволяет не только освоить теоретические знания, но и развить практические навыки принятия решений в условиях ограниченного времени и под давлением. Активное участие педагога в учебном процессе обеспечивает индивидуальный подход к каждому обучающемуся и позволяет оперативно корректировать образовательный маршрут в зависимости от достигнутых результатов. ВОС стирает границы между искусством, театром и образованием, создавая условия для всестороннего развития будущих специалистов в области информационной безопасности.

Основная часть

В настоящее время наблюдается активный интерес к исследованию потенциала ВОС. Например, авторы [1] углубленно изучают возможные психофизиологические и физиологические реакции обучающихся, возникающие в процессе их погружения в виртуальную реальность (ВР). Они также предлагают перспективный подход, заключающийся в сочетании виртуальной и дополненной реальности для создания еще более интерактивных и эффективных образовательных сред. Вопросы создания виртуальной среды для изучения базовых дисциплин также активно исследуются. Так, авторы рассматривают применение ВР в процессе обучения иностранным языкам, химии, в освоении физики. Данные исследования демонстрируют широкие возможности ВР для трансформации традиционных образовательных процессов и создания новых, более эффективных и увлекательных форм обучения.

Виртуальная реальность в обучении

Большой потенциал для развития и совершенствования образовательных процессов демонстрирует применение цифрового обучения при освоении прикладных дисциплин и повышении квалификации специалистов различных областей. Существуют многочисленные исследования, посвященные созданию виртуальной среды для обучения операторов роботов, практикующих врачей, операторов транспортных средств и пожарных [7]. Эти примеры наглядно демонстрируют, как ВР может быть эффективно использована для имитации реальных ситуаций и отработки практических навыков. Однако, несмотря на очевидные преимущества, вопросы формирования ВОС для изучения информационной безопасности и кибератак остаются недостаточно исследованными. В то же время современные реалии характеризуются острой потребностью в высококвалифицированных специалистах в области информационной безопасности, что делает данное направление крайне актуальным.

Для создания эффективной ВОС, ориентированной на изучение информационной безопасности, предлагается использовать данные имитаторы. Эти инновационные системы позволяют моделировать реальные цифровые атаки в контролируемых условиях, предоставляя обучающимся уникальную возможность отработать навыки обнаружения и нейтрализации угроз. Данные модули, по сути, являются высокотехнологичными тренажерами, которые создают реалистичные сценарии атак, имитируя действия злоумышленников. Благодаря гибкой настройке параметров и автоматизации процессов на этих системах можно проводить многократные тренировки, постепенно усложняя

сценарии и повышая уровень сложности задач. Использование данных комплексов в образовательном процессе позволяет существенно повысить эффективность обучения, сократить временные и финансовые затраты на подготовку специалистов в области информационной безопасности.

Моделирование, или эмуляция злоумышленников представляет собой процесс искусственного воссоздания действий, характерных для реальных киберпреступников, с целью всесторонней оценки устойчивости информационной системы организации. По сути, это своего рода симуляция кибератаки, которая позволяет выявить уязвимости и просчеты в системе безопасности до того, как ими воспользуются злоумышленники. Несмотря на то, что на первый взгляд моделирование атак может показаться схожим с автоматизированным тестированием на проникновение, оно охватывает гораздо более широкий спектр аспектов информационной безопасности. Задача такого моделирования заключается не только в обнаружении уязвимостей, но и в определении наиболее вероятных путей атаки, которые может выбрать злоумышленник [7]. Это позволяет организации не только устранить наиболее критичные угрозы, но и разработать комплексный план реагирования на инциденты, оптимизировать распределение ресурсов безопасности и в конечном итоге минимизировать риски кибератак. Моделирование злоумышленников выступает как мощный инструмент организаций для проактивной защиты информационной безопасности, опережая на шаг потенциальные угрозы.

Большинство современных инструментов и платформ, предназначенных для моделирования цифровых атак, предлагают автоматизированные или полуавтоматизированные механизмы для получения детального представления о сетевой инфраструктуре потенциальной жертвы [5]. Фактически такие инструменты позволяют симулятору атаки эффективно собирать информацию о различных аспектах целевой сети, включая ее топологию, используемые протоколы, установленные сервисы, конфигурацию устройств и другие критически важные данные. Полученная информация в дальнейшем используется для построения реалистичной модели атаки, которая учитывает специфические особенности защищаемой сети. Инструменты предоставляют специалистам по информационной безопасности мощный инструмент для оценки уязвимостей и выявления потенциальных векторов атак, что дает возможность принимать более обоснованные решения в области обеспечения кибербезопасности.

Применение данных систем в процессе создания ВОС открывает перед обучающимися уникальные возможности для приобретения практических навыков, необходимых для успешной работы в сфере информационной безопасности. Погружаясь в реалистичную виртуальную среду, имитирующую реальные условия кибератак, обучающиеся могут оттачивать свои навыки обнаружения и нейтрализации угроз, разрабатывать эффективные стратегии защиты информации и принимать взвешенные решения в условиях ограниченного времени и под давлением. Регулярные тренировки в такой среде формируют устойчивые профессиональные алгоритмы действий, что является ключевым фактором для успешного противодействия цифровым угрозам [1]. Кроме того, виртуальная среда способствует развитию психологической устойчивости и готовности к принятию самостоятельных решений в сложных и нестандартных ситуациях, что является неотъемлемой частью работы специалиста в области информационной безопасности. Применение таких имитаторов в образовательном процессе позволяет подготовить высококвалифицированных специалистов, способных эффективно противостоять современным киберугрозам и обеспечить надежную защиту информационных ресурсов организаций.

Программируемые имитаторы

Реализация этого направления предполагает использование специальных программных инструментов, называемых имитаторами. При этом создание системы имитации кибератак может осуществляться двумя основными способами: путем применения готовых программных решений или путем разработки собственных программируемых имитаторов [6]. К числу наиболее популярных готовых решений относятся такие программы, как MITRE Caldera, Atomic Red Team, DumpsterFire, Firedrill и InfectionMonkey [7]. Каждая из этих программ обладает своими уникальными возможностями и функционалом, что позволяет выбрать оптимальное решение в зависимости от конкретных потребностей организации.

Применение мониторинговых компьютерных атак преследует цель комплексного решения ряда задач, направленных на повышение уровня безопасности критически важных инфраструктур [8].

- Во-первых, такие имитаторы позволяют проводить глубокий анализ системы управления, выявляя скрытые уязвимости и потенциальные точки проникновения для злоумышленников.
- Во-вторых, использование имитаторов дает возможность оценить весь спектр угроз, с которыми может столкнуться система, и спрогнозировать возможные действия злоумышленников при реализации различных типов атак.
- В-третьих, имитаторы позволяют провести всестороннюю оценку эффективности средств защиты, включая автоматизированные рабочие места, серверы сбора

данных, системы электронной почты, средства предупреждения компьютерных атак и другие компоненты системы безопасности, что позволяет выявить слабые звенья и оптимизировать конфигурацию защитных механизмов.

- В-четвертых, с помощью имитаторов можно провести комплексную оценку устойчивости функционирования всей системы в условиях реальных кибератак, что позволяет оценить эффективность разработанных методов и алгоритмов противодействия и внести необходимые корректировки в систему защиты.

Использование данных имитаторов компьютерных атак является одним из наиболее эффективных способов обеспечения безопасности критически важных инфраструктур, позволяя выявить и устранить уязвимости до того, как ими воспользуются злоумышленники.

Применение специализированного программного и аппаратного обеспечения в учебном процессе, базирующееся на создании стендовых полигонов в специально оборудованных аудиториях, открывает широкие возможности для решения множества образовательных задач [4].

- Во-первых, такие полигоны предоставляют студентам уникальную возможность получить практический опыт работы с современными информационными системами и технологиями в условиях, максимально приближенных к реальным.
- Во-вторых, стендовые полигоны позволяют моделировать различные сценарии работы информационных систем, что способствует глубокому пониманию студентами принципов их функционирования и взаимодействия.
- В-третьих, использование стендовых полигонов способствует развитию у студентов навыков самостоятельного решения проблем, анализа и принятия решений в условиях ограниченного времени и наличия большого объема информации.
- В-четвертых, стендовые полигоны позволяют проводить различные эксперименты и исследования, что стимулирует творческую активность студентов и способствует развитию их исследовательских навыков.

В целом, использование стендовых полигонов в учебном процессе позволяет существенно повысить эффективность обучения и подготовить высококвалифицированных специалистов, способных успешно работать в сфере информационных технологий.

Обучение студентов техническим аспектам информационной безопасности, направленное на эффективное противодействие компьютерным атакам, предполагает глубокое погружение в практическую составляющую данной области. Студенты получают уникальную возможность освоить широкий спектр инструментов и программ, которые активно используются злоумышленниками для проведения кибератак различной сложности. Подход позволяет будущим специалистам по информационной безопасности не только теоретически понимать принципы функционирования этих инструментов, но и на практике отрабатывать навыки их обнаружения, анализа и нейтрализации. В результате студенты приобретают ценный опыт эффективно противостоять реальным киберугрозам и разрабатывать надежные системы защиты информации.

Использование стендовых полигонов с имитаторами компьютерных атак в учебном процессе позволяет студентам не только осваивать существующие средства защиты информационных систем, но и активно участвовать в их совершенствовании. Студенты получают возможность проводить всестороннее тестирование существующих средств защиты, моделируя различные сценарии атак и оценивая их эффективность в реальных условиях. Подход позволяет выявить скрытые уязвимости в системе безопасности и разработать рекомендации по их устранению. При этом работа со стендовыми полигонами стимулирует творческую активность студентов и способствует развитию у них навыков разработки новых средств защиты, способных противостоять современным и перспективным видам кибератак. Использование имитаторов компьютерных атак в учебном процессе не только готовит высококвалифицированных специалистов в области информационной безопасности, но и способствует развитию новых технологий и методов защиты информации [7].

Использование имитаторов хакерских атак в учебном процессе не только повышает уровень подготовки будущих специалистов, но и открывает широкие перспективы для сотрудничества с представителями индустрии информационной безопасности. Взаимодействие с производителями средств защиты информационных систем, основанное на совместной работе со студентами над реальными проектами, позволяет не только продемонстрировать высокий уровень подготовки выпускников, но и привлечь внимание индустрии к инновационным решениям, разработанным в рамках учебного процесса. Такое сотрудничество способствует созданию синергетического эффекта, когда опыт и знания представителей академической среды дополняются практическими потребностями и экспертизой индустриальных партнеров. В результате совместных исследований и разработок появляются новые эффективные средства защиты информации, способные противостоять самым современным киберугрозам. Кроме того, сотрудничество с индустрией позволяет студентам получить ценный опыт работы над реальными проектами, что значительно повышает их конкурентоспособность на рынке труда.

Можно отметить, что применение таких имитаторов в сочетании с созданием специализированных стендовых полигонов предоставляет уникальную возможность для глубокой проработки и оценки эффективности методов противодействия кибератакам в условиях, максимально приближенных к реальным, с особым акцентом на критически важные инфраструктуры. Эти инновационные подходы позволяют не только моделировать различные сценарии таких атак, но и проводить детальный анализ реакции защитных систем, выявляя их сильные и слабые стороны. При этом такие имитаторы атак активно используют компьютерные сети в качестве полигонов для программного моделирования, что обеспечивает максимально реалистичные условия для тестирования средств защиты. В качестве таких сетей могут выступать как реальные производственные сети, так и искусственно созданные модели, точно воспроизводящие архитектуру и функциональность реальных систем.

Заключение

Развертывание стендовых полигонов, призванных обеспечить полноценную ВОС для углубленного изучения кибератак, требует значительных финансовых вложений, что зачастую становится непреодолимым препятствием для большинства образовательных учреждений. Однако следует отметить, что для успешной реализации подобных проектов представляется целесообразным привлечение к сотрудничеству ведущих вендоров программного обеспечения на основе заключения долгосрочных договоров о стратегическом партнерстве. Это открывает перед образовательными организациями ряд существенных преимуществ.

- Во-первых, данные субъекты, заинтересованные в развитии рынка информационной безопасности, как правило, готовы предоставить образовательным учреждениям значительные скидки на программное обеспечение, а также оказать техническую поддержку при его внедрении и настройке.
- Во-вторых, такое сотрудничество позволяет получить доступ к самым современным технологиям и решениям в области цифровой безопасности, что позволяет создать максимально реалистичную и актуальную образовательную среду.
- В-третьих, совместная работа способствует формированию у студентов практических навыков работы с продуктами ведущих мировых производителей, что повышает их конкурентоспособность на рынке труда.

Сотрудничество с компаниями, специализирующимися на разработке и производстве передовых цифровых имитаторов компьютерных атак (BAS)[2], открывает перед образовательными организациями широкие перспективы для создания высокоэффективных виртуальных полигонов. Компании обладают уникальными экспертными знаниями в области кибербезопасности и могут предоставить образовательным учреждениям не только доступ к новейшим технологиям и продуктам, но и оказать всестороннюю поддержку в процессе их внедрения и адаптации к специфическим потребностям учебного процесса. В частности, компании-разработчики могут помочь в обучении преподавателей, обеспечивая их необходимыми методическими материалами и проводя специализированные тренинги. Кроме того, сотрудничество с вендорами позволяет образовательным организациям быть в курсе последних тенденций в области цифровой безопасности и адаптировать учебные программы в соответствии с меняющимися требованиями рынка. При этом партнерство с компаниями, специализирующимися на разработке данных систем, является одним из ключевых факторов успешной реализации проектов по созданию ВОС для подготовки высококвалифицированных специалистов в области информационной безопасности.

Создание совместной научно-исследовательской лаборатории, ориентированной на разработку и апробацию инновационных методов и показателей оценки эффективности противодействия хакерским атакам, представляющим угрозу для критически важной инфраструктуры, открывает перед образовательными организациями и индустриальными партнерами широкие перспективы для совместной работы. В рамках такой лаборатории становится возможным проведение углубленных исследований в области кибербезопасности, направленных на выявление новых уязвимостей и разработку эффективных мер противодействия киберугрозам. Более того, лаборатория может стать площадкой для создания и тестирования прототипов новых систем защиты, основанных на использовании передовых технологий и алгоритмов. Применение инструментов, необходимых для моделирования различных сценариев кибератак, позволяет проводить реалистичные испытания разрабатываемых решений и оценивать их эффективность в условиях, максимально приближенных к реальным. Создание совместной научно-исследовательской лаборатории не только способствует повышению уровня научных исследований в области цифровой безопасности, но и ускоряет процесс внедрения инновационных решений в практику, что в конечном итоге повышает уровень защищенности критически важной инфраструктуры.

[2] По данным специалистов в области информационной безопасности, рынок BAS в России только формируется и составляет порядка 2–2,5 млн долларов США в годовом выражении. — *Примеч. ред.*

Организация специализированных обучающих курсов и тренингов для сотрудников и студентов, посвященных практическому использованию цифровых имитаторов атак, представляет собой стратегически важное направление развития любой организации, стремящейся обеспечить высокий уровень защищенности своих информационных ресурсов. Такие курсы позволяют не только повысить уровень осведомленности сотрудников о современных киберугрозах, но и развить у них практические навыки обнаружения и нейтрализации различных видов атак. Студенты, прошедшие подобные тренинги, получают возможность освоить передовые технологии в области кибербезопасности и приобрести ценный опыт работы с профессиональными инструментами, что значительно повышает их конкурентоспособность на рынке труда. Кроме того, организация обучающих мероприятий способствует созданию внутри компании атмосферы непрерывного обучения и профессионального развития, что является одним из ключевых факторов успеха в условиях постоянно меняющейся цифровой среды.

Сотрудничество с другими образовательными учреждениями и научно-исследовательскими центрами, специализирующимися в данной области, открывает перед участниками широкие возможности для совместного развития и достижения синергетического эффекта. Такое взаимодействие способствует активному обмену знаниями, опытом и лучшими практиками в области обеспечения информационной безопасности, что позволяет участникам сотрудничества не только расширить собственные компетенции, но и получить доступ к уникальным ресурсам и технологиям, разработанным в других организациях. Совместные исследовательские проекты, направленные на изучение новых угроз кибербезопасности и разработку инновационных методов защиты, позволяют создавать научные продукты, отвечающие самым высоким мировым стандартам. Кроме того, проведение совместных мероприятий, таких как конференции, семинары и хакатоны, способствует укреплению профессиональных связей между участниками сотрудничества и созданию благоприятной среды для обмена идеями и опытом. Сотрудничество с другими образовательными учреждениями и научно-исследовательскими центрами является одним из наиболее эффективных способов ускорения темпов развития науки и образования в области кибербезопасности, что в конечном итоге способствует повышению уровня защищенности информационных систем и инфраструктуры.

Применение программируемых имитаторов хакерских атак в образовательном процессе способствует формированию инновационной ВОС, которая открывает перед студентами и преподавателями уникальные возможности для глубокого погружения в реальный мир кибербезопасности и выводит образовательный процесс в области информационной безопасности на качественно новый уровень, обеспечивая формирование востребованных профессиональных компетенций [7]. Симуляция различных сценариев кибератак дает студентам наглядно понять принципы действия злоумышленников, научиться выявлять уязвимости в информационных системах, разрабатывать эффективные стратегии предотвращения и реагирования на инциденты информационной безопасности, а также проводить тестирование и отладку собственных средств защиты.

Применение данных модулей в образовательном процессе представляет собой инновационный подход, позволяющий не только эффективно проверять устойчивость компьютерных сетей и других информационных систем к широкому спектру современных киберугроз, но и разрабатывать эффективные методы противодействия им. Имитаторы создают контролируемую среду, в которой студенты и специалисты могут оттачивать свои навыки в обнаружении и нейтрализации различных видов атак, не рискуя при этом нанести ущерб реальным системам. Однако важно подчеркнуть, что использование таких инструментов должно осуществляться исключительно в образовательных целях и при строгом соблюдении законодательства, а также с согласия соответствующих организаций. Для создания полноценной ВОС среды, оснащенной современными имитаторами кибератак, целесообразно привлекать к сотрудничеству ведущих производителей программного обеспечения. Заключение долгосрочных соглашений о стратегическом партнерстве с такими компаниями позволяет образовательным учреждениям получить доступ к новейшим технологиям и продуктам, а также обеспечить необходимую техническую поддержку. Кроме того, сотрудничество с вендорами способствует формированию у студентов практических навыков работы с профессиональными инструментами, что повышает их конкурентоспособность на рынке труда.

ВОС, построенная на фундаментальном использовании передовых технологий имитации компьютерных атак, открывает перед современным образованием в сфере информационной безопасности совершенно новые горизонты и позволяет достичь беспрецедентного уровня качества подготовки специалистов, способных эффективно противостоять сложнейшим киберугрозам, характерным для стремительно развивающейся цифровой эпохи. Такая среда обеспечивает уникальную возможность для глубокого погружения в реальные сценарии кибератак, что способствует формированию у студентов не только прочных теоретических знаний, но и практических навыков, необходимых для успешной работы в области цифровой без-

опасности. Имитаторы позволяют моделировать широкий спектр киберугроз, от простых фишинговых до сложных целенаправленных атак, что позволяет студентам развить критическое мышление, научиться выявлять уязвимости в информационных системах, разрабатывать эффективные стратегии защиты и проводить тестирование собственных решений. ВОС, основанная на данных системах, не только повышает уровень подготовки будущих специалистов, но и способствует развитию отечественной системы безопасности в целом.

Литература

1. *Krasilnikova T.K., Egorov G.G., Derkacheva T.V.* The use of modern digital technologies in the implementation of the rights and legitimate interests of citizens // Lecture Notes in Networks and Systems (см. в книгах). 2021. Т. 155. С. 1118–1125.

2. *Shubenkova K., Egorov G.G.* Legal and technical forms of developing digital law-enforcement in modern Russia: problems and prospects // Lecture Notes in Networks and Systems (см. в книгах). 2020. Т. 111. С. 705–711.

3. *Блохин Б.М.* Иммерсивные симуляционные технологии обучения практикующих врачей навыкам сердечно-легочной реанимации детям // Вестник терапевта. 2018. № 7 (31). С. 4–11.

4. *Егоров Г.Г., Дубовикова Е.М.* Проектное планирование в современном образовании // Вестник Воронежского государственного университета инженерных технологий. 2022. № 1 (91). С. 356–364.

5. *Прибылова Н.Г.* Иммерсионное обучение иностранному языку в зарубежных странах // Психология образования в поликультурном пространстве. 2016. № 2 (34). С. 95–100.

6. *Хороших П.П.* Иммерсивные образовательные среды: психофизиологический аспект // Психология и психотехника. 2021. № 1. С. 78–88. DOI: 10.7256/2454-0722.2021.1.34819

7. *Швырев Б.А., Тищенко Ю.Ю.* Кибератаки: иммерсионная образовательная среда и ее формирование // Уголовно-исполнительная система: право, экономика, управление. 2024. № 1. С. 30–33.

8. *Юсупов А.А.* Исследование человеческого фактора в обучении пожарных с погружением в виртуальную реальность // Современная наука: актуальные вопросы, достижения и инновации: материалы XXIX Международной научно-практической конференции (г. Пенза, 10 февраля 2023 г.): сб. научных статей / отв. ред. Г.Ю. Гуляев. Пенза: Наука и просвещение, 2023. С. 260–262.

References

1. *Krasilnikova, T.K., Egorov, G.G., Derkacheva, T.V.* The use of modern digital technologies in the implementation of the rights and legitimate interests of citizens. *Lecture Notes in Networks and Systems* (see in books). 2021. Vol. 155. P. 1118–1125.

2. *Shubenkova, T.K., Egorov, G.G.* Legal and technical forms of developing digital law-enforcement in modern Russia: problems and prospects. *Lecture Notes in Networks and Systems* (see in books). 2020. Vol. 111. P. 705–711.

3. *Blokhin, B.M.* Immersive simulation technologies for teaching practicing doctors cardiopulmonary resuscitation skills to children. *Vestnik of the therapist.* 2018. No. 7 (31). P. 4–11.

4. *Egorov, G.G., Dubovikova, E.M.* Project planning in modern education. *Vestnik of the Voronezh State University of Engineering Technologies*. 2022. No. 1 (91). P. 356–364.

5. *Pribylova, N.G.* Immersion teaching of a foreign language in foreign countries. *Psychology of education in a multicultural space*. 2016. No. 2 (34). P. 95–100.

6. *Khoroshikh, P.P.* Immersive educational environments: psychophysiological aspect. *Psychology and psychotechnics*. 2021. No. 1. P. 78–88. DOI: 10.7256/2454-0722.2021.1.34819

7. *Shvyrev, B.A., Tishchenko, Yu.Yu.* Cyberattacks: immersion educational environment and its formation. *Penal system: law, economics, management*. 2024. No. 1. P. 30–33.

8. *Yusupov, A.A.* Study of the human factor in training firefighters with immersion in virtual reality. *Modern science: current issues, achievements and innovations*: Proceedings of the XXIX International scientific and practical conference (Penza, February 10, 2023): Collection of scientific articles / ed. by G.Yu. Gulyaev. Penza: Science and Education, 2023. P. 260–262.