- ОБРАЗОВАНИЕ В РОССИИ И МИРЕ -

Дата поступления рукописи в редакцию: 02.04.2026 г. DOI: 10.24412/2782-3830-2026-7-526-530
Дата принятия рукописи в печать: 13.07.2026 г.

ШВЫРЕВ Борис Анатольевич,
ведущий научный сотрудник
Института проблем передачи информации
Российской академии наук имени А.А. Харкевича (ИППИ РАН),
кандидат физико-математических наук, доцент,
e-mail: e-maili@bor2275.ru

ТИЩЕНКО Юрий Юрьевич,
ведущий научный сотрудник ФКУ
НИИ ФСИН России,
кандидат юридических наук,
e-mail: yutish@list.ru

ИЗУЧЕНИЕ КИБЕРАТАК И ФОРМИРОВАНИЕ ИММЕРСИОННОЙ ОБРАЗОВАТЕЛЬНОЙ СРЕДЫ

Аннотация. *В статье рассматриваются особенности формирования иммерсионной образовательной среды с использованием управляемого имитатора компьютерных атак. Рассматривается использование управляемого имитатора компьютерных атак в качестве метода обучения студентов дисциплинам, связанным с информационной безопасностью. Данный инструмент позволяет имитировать различные виды атак на информационную систему и проводить тренировки для повышения навыков по ее защите. Иммерсионная образовательная среда в области информационной безопасности – позволяет реализовать принцип интерактивного обучения с нелинейным сценарием обучения и вовлеченности в процесс педагога и обучающегося с использованием информационных технологий. Использование управляемых имитаторов позволяет обеспечить проверку устойчивости компьютерных вычислительных сетей и других систем к продвинутым кибератакам и разработать эффективные методы борьбы с ними. Для организации такой иммерсионной образовательной среды целесообразно привлекать производителей программного обеспечения на принципах стратегического партнерства.*

Ключевые слова: *Иммерсионная образовательная среда, управляемый имитатор компьютерных атак, образовательный процесс, информационная безопасность.*

SHVYREV Boris Anatolyevich,
leading Researcher at the A.A. Kharkevich
Institute for Information Transmission Problems
of the Russian Academy of Sciences (IPPI RAS),
Candidate of Physical and Mathematical Sciences,
Associate Professor

TISHCHENKO Yuri Yurievich,
leading researcher, Federal State Institution Research Institute
of the Federal Penitentiary Service of Russia,
Moscow, Russian Federation;
Candidate of Legal Sciences

STUDYING CYBERATTACKS AND CREATING AN IMMERSIVE EDUCATIONAL ENVIRONMENT

Annotation. *The article discusses the features of the formation of an immersion educational environment using a controlled simulator of computer attacks. The use of a controlled simulator of*

computer attacks as a method of teaching students disciplines related to information security is considered. This tool allows you to simulate various types of attacks on an information system and conduct training to improve its protection skills. Immersion educational environment in the field of information security – allows you to implement the principle of interactive learning with a nonlinear learning scenario and involvement in the process of the teacher and the student using information technology. The use of controlled simulators makes it possible to check the stability of computer networks and other systems to advanced cyber attacks and develop effective methods to combat them. To organize such an immersive educational environment, it is advisable to involve software manufacturers on the principles of strategic partnership.

Key words*: Immersion educational environment, controlled simulator of computer attacks, educational process, information security.*

Современная информационная среда требует от всех ее участников не только умения пользоваться компьютерами и сетями, но и знания основ информационной безопасности. К сожалению, далеко не все пользователи понимают важность защиты своих данных и часто не обладают достаточными знаниями, чтобы защитить свои устройства от различных угроз. Поэтому важно, чтобы специалисты в области информационной безопасности имели навыки работы с реальными уязвимостями и могли оперативно реагировать на возникающие угрозы.

Одним из инструментов, позволяющих получить практический опыт в работе с реальными уязвимостями в живую, погрузится в информационные процессы, является управляемый имитатор компьютерных атак. Данный инструмент позволяет имитировать различные виды атак на информационную систему и проводить тренировки для повышения навыков по ее защите. Иммерсионная образовательная среда – это новая форма обучения, вовлекающая обучающегося в образовательный процесс, имитирующий реальные ситуационные условия, организованный так, что обучающийся является важным элементов динамического нелинейного образовательного процесса. Реализация обучения в предметах по кибербезопасности имеет ряд трудностей, связанных со сложностью используемого программного продукта, сложных сценариев занятий, при упрощении которых теряется суть и интерес у обучающихся, а также главная сложность заключает в большой динамичности предметной области в информационной безопасности. Иногда работы по реализации информационной безопасности, решение по защите информации и противодействие угрозам и уязвимостям на реальных сложных объектах называют – «искусством». Одним из современных методов, стирающих грань между искусством, театром и образованием является технология иммерсионного обучения. Иммерсионная образовательная среда в области информационной безопасности – позволяет реализовать принцип интерактивного обучения с нелинейным сценарием обучения и вовлеченности в процесс педагога и обучающегося с использованием информационных технологий.

В настоящее время применение иммерсионной образовательной среды активно изучается, так в [1] авторы обсуждают возможные психофизиологические и физиологические реакций обучающегося в процессе его погружения в иммерсионную среду, и они предлагают совмещать виртуальную и дополненную реальность. Вопросы формирования иммерсионной среды при изучении базовых предметов образовательного процесса рассмотрены в [2] для изучения иностранных языков, в [3] для изучения химии и в [4] для изучения физики. Большим потенциалом обладает реализация иммерсионного обучения при освоении прикладных предметов, при повышении квалификации специалистов. Так известны работы, в которых обсуждается создание иммерсионной среды для обучения операторов роботов [5], практикующих врачей [6], операторов транспортных средств [7], пожарных [8]. Однако вопросам формирования иммерсионной образовательной среды для изучения информационной безопасности и кибератак внимание уделено недостаточно, хотя потребность в изучении этого направления продиктована реалиями наших дней с высокой востребованностью в высококвалифицированных специалистов в области информационной безопасности. Для реализации иммерсионной образовательной среды для изучения информационной безопасности воспользуемся управляемыми имитаторами. Управляемые имитаторы - это системы моделирования кибератак, позволяющие произвести симуляцию реального взлома, атаки на инфраструктуру в автоматическом контролируемом режиме.

Моделирование или эмуляция злоумышленников - это процесс имитации поведения злоумышленника. Он предлагает возможность проверить устойчивость организации к продвинутым злоумышленникам в ситуации, известной как предполагаемое нарушение, т.е. все симуляции выполняются системой добровольно. Хотя имитация злоумышленников на первый взгляд очень

похожа на автоматическое тестирование на проникновение, этот тип моделирования охватывает более широкий спектр инфраструктуры безопасности. Задача состоит в том, чтобы определить различные пути атаки, которые может предпринять противник, устранить наиболее серьезные угрозы и расставить приоритеты с помощью действенного плана исправления, чтобы максимально использовать ресурсы безопасности и снизить киберриски.

Большинство инструментов и платформ для моделирования атак предоставляют автоматические или полуавтоматические способы получения представления злоумышленника о сети жертвы [9]. Применение управляемых имитаторов для формирования иммерсионной образовательной среды позволяет обучающемуся получить практические навыки работы в реальных условиях информационного противодействия, сформировать устойчивые профессиональные алгоритмы принятия решений, получить психологическую подготовку к принятию решений в сложных практических задачах и сформировать готовность к самостоятельным профессиональным действия в области информационной безопасности. Рассмотрим одно из направлений информационной безопасности по противодействию кибератакам [10]. Применение имитаторов может базироваться на готовых решениях и программах либо на создании собственных управляемых имитаторов [11].К готовым решениям относятся такие программы как:

1. MITRE CALDERA
2. Atomic Red Team
3. DumpsterFire
4. Firedrill
5. InfectionMonkey

Использование контролируемых имитаторов компьютерных атак [12] имеет целью решение нескольких задач, связанных с обеспечением безопасности критически важной инфраструктуры:

– обнаружение уязвимостей в системе управления;
– оценка возможностей злоумышленников при реализации угроз компьютерных атак;
– агрегированная оценка динамики процессов использования средств защиты, включающая автоматизированные рабочие места, серверы сбора данных и электронную почту, средства предупреждения компьютерных атак и другие компоненты;
– комплексная оценка устойчивости функционирования системы в условиях компьютерных атак на основе разработанных методов и алгоритмов противодействия.

Применение программного и аппаратного обеспечения в учебном процессе основано на использовании стендовых полигонов в специальных аудиториях, что позволяет решать следующие задачи:

1. Обучение студентов техническим аспектам информационной безопасности, позволяющим эффективно бороться с компьютерными атаками. Студенты могут получить практические навыки работы с различными инструментами и программами, используемыми злоумышленниками для проведения атак на информационные системы.
2. Тестирование средств защиты информационных систем. Использование имитаторов компьютерных атак позволяет проверить эффективность существующих средств защиты, выявить и устранить уязвимости в системе.
3. Разработка новых средств защиты. Обучение студентов работе с имитаторами компьютерных атак может стать стимулом для разработки новых средств защиты, которые будут более эффективно справляться с новыми видами атак.
4. Сотрудничество с индустрией. Работа с имитаторами кибератак может привлечь внимание индустрии к образовательным организациям и позволить установить контакты с производителями средств защиты, что может привести к плодотворному сотрудничеству в области исследований и разработок новых средств противодействия.

Таким образом, использование управляемых имитаторов кибератак и стендовых полигонов позволяет осуществить отработку методов и показателей оценки эффективности противодействия кибератакам на критически важной инфраструктуре в практических условиях. Управляемые имитаторы кибератак используют компьютерные сети для проведения модели нападения на них. Это могут быть реальные компьютерные сети либо искусственно созданные сети, которые имитируют реальные. Развертывание таких стендовых полигонов требует большого бюджета для реализации, что обычно останавливает образовательные организации от реализации иммерсионной образовательной среды, но стоит отметить, что для реализации таких проектов целесообразно приглашать самих вендоров программного обеспечения на основе заключения договоров о стратегическом партнерстве. Выделим следующие варианты стратегического партнерства в вопросах формирования иммерсионной образовательной среды для изучения кибератак:

– Сотрудничество с компаниями, специализирующимися на разработке и производстве управляемых имитаторов компьютерных атак. Такие компании могут предоставить образовательной организации доступ к своим продуктам и технологиям, а также помочь в обучении преподавателей.
– Создание совместной научно-исследовательской лаборатории по разработке и отработке методов и показателей оценки эффективности противодействия кибератакам на критически важной инфраструктуре. В рамках такой лаборатории можно будет проводить исследования в области кибербезопасности, разрабатывать новые методы защиты от компьютерных атак и тестировать их на управляемых имитаторах.
– Организация обучающих курсов и тренингов для своих сотрудников, студентов, по темам кибербезопасности и использованию управляемых имитаторов компьютерных атак. Это позволит повысить компании квалификацию своих сотрудников и улучшить их профессиональную подготовку, а также повысит готовность студентов к вхождению в профессию.
– Сотрудничество с другими образовательными учреждениями и научно-исследовательскими центрами в области кибербезопасности и тестирования компьютерных систем на управляемых имитаторах. Такое сотрудничество позволит обмениваться знаниями и опытом, а также проводить совместные исследования в области кибербезопасности и тестирования.

Заключение

Применение управляемых имитаторов кибератак в образовательном процессе формирует иммерсионную образовательную среду и выводит образовательный процесс в области информационной безопасности на новый уровень формирования профессиональных компетенций. Обучение в такой среде позволяет понять принципы работы злоумышленников, научиться выявлять и предотвращать атаки на инфраструктуру, а также разрабатывать и тестировать собственные средства противодействия компьютерным атакам.

Использование управляемых имитаторов позволяет обеспечить проверку устойчивости компьютерных вычислительных сетей и других систем к продвинутым кибератакам и разработать эффективные методы борьбы с ними. Однако, необходимо учитывать, что такие имитаторы могут использоваться только в образовательных целях и с согласия соответствующих организаций. Для организации такой иммерсионной образовательной среды целесообразно привлекать производителей программного обеспечения на принципах стратегического партнерства. Иммерсионная образовательная среда, основанная на использовании управляемых имитаторов компьютерных атак в образовательном процессе, может существенно улучшить качество обучения и подготовку студентов к борьбе с киберугрозами, что является важным направлением развития систем безопасности в цифровую эпоху.

Список литературы

[1] Хороших П.П. Иммерсивные образовательные среды: психо-физиологический аспект / П.П.Хороших, А.А.Сергиевич, Т.А. Баталова // Психология и Психотехника. – 2021. – № 1. DOI: 10.7256/2454-0722.2021.1.34819 URL:https://nbpublish.com/library_read_article.php?id=34819

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

[3] Курушкин М.В.Айтрекинг в иммерсивной виртуальной реальности: персонализация образовательных траекторий в химическом образовании / М.В.Курушкин // НИР: грант № 20-78-10135. Российский научный фонд. 2020.

[4] Кирюхина Н.В.Иммерсивные технологии в обучении физике / Н.В. Кирюхина, Н.А. Плеханова // Проблемы современного педагогического образования. 2023. № 79-2. С. 133-136.

[5] Жердева Л.А. Навигация наземного робота с использованием глубокого обучения с подкреплением в иммерсивной среде / Л.А.Жердева, А.Жердев, Е.Ю.Минаев // В сборнике: Информационные технологии и нанотехнологии (ИТНТ-2021). Сборник трудов по материалам VII Международной конференции и молодежной школы. Самара, 2021. С. 34062.

[6] Блохин Б.М. Иммерсивные симуляционные технологии обучения практикующих врачей навыкам сердечно-легочной реанимации детям / Б.М.Блохин, И.В.Гаврютина, В.Ю.Стешин, Е.Ю.Овчаренко, И.П.Лобушкова// Вестник терапевта. 2018. № 7 (31). С. 4-11.

[7] Карелина М.В. Методические аспекты применения тренажеров с иммерсивной технологией при обучении в университете транспорта / М.В.Карелина, С.П.Вакуленко, П.А.Егоров, О.В.Мерецков // Отечественная и зарубежная педагогика. 2021. Т. 2. № 6 (81). С. 64-80.

[8] Юсупов А.А. Исследование человеческого фактора в обучении пожарных с погружением в виртуальную реальность / Юсупов А.А. // В сборнике: Современная наука: актуальные

вопросы, достижения и инновации. сборник статей XXIX Международной научно-практической конференции. Пенза, 2023. С. 260-262.

[9] Волков С.Д., Царегородцев А.В. Один из подходов к обеспечению защиты от компьютерных атак при реализации информационной функции государства на внутреннем уровне // Вестник Пермского национального исследовательского политехнического университета. Электротехника, информационные технологии, системы управления. 2020. № 36. С. 159-174.

[10] Климов С.М. Методы и модели противодействия компьютерным атакам. Люберцы: КАТАЛИТ, 2008. СС. 64-64.

[11] Волков С.Д. Обзор подходов к построению систем обнаружения компьютерных атак для информационно-телекоммуникационных систем, функционирующих на основе технологии облачных вычислений // Collegium Linguisticum - 2017. Материалы ежегодной конференции студенческого научного общества МГЛУ. 2017. М.: ФГБОУ ВО МГЛУ. С. 442-447.

[12] Степашкин М.В., Котенко И.В., Богданов В.С. Моделирование атак для активного анализа уязвимостей компьютерных сетей // Вторая всероссийская научнопрактическая конференция по имитационному моделированию и его применению в науке и промышленности «Имитационное моделирование. Теория и практика» ИММОД–2020. С. 269–273.

References

[1] Khoroshikh P.P. Immersive educational environments: psycho-physiological aspect/P.P. Khoroshikh, A.A. Sergievich, T.A. Batalova//Psychology and Psychotechnics. – 2021. – № 1. DOI: 10.7256/2454-0722.2021.1.34819 URL:https://nbpublish.com/library_read_article.php?id=34819

[2] Pribylova N.G. Immersion foreign language education in foreign countries/N.G. Pribylova//Psychology of education in a multicultural space. 2016. № 2 (34). S. 95-100.

[3] Kurushkin M.V. Tracking in immersive virtual reality: personalization of educational trajectories in chemical education/M.V. Kurushkin//Research: grant No. 20-78-10135. Russian Science Foundation. 2020.

[4] Kiryukhina N.V. Immersive technologies in teaching physics/N.V. Kiryukhina, N.A. Plekhanova// Problems of modern pedagogical education. 2023. № 79-2. S. 133-136.

[5] Zherdeva L.A. Navigation of a ground robot using deep learning with reinforcement in an immersive environment/L.A. Zherdeva, A. Zherdev, E. Yu. Minaev//In the collection: Information Technologies and Nanotechnology (ITNT-2021). Collection of works based on the materials of the VII International Conference and Youth School. Samara, 2021. P. 34062.

[6] Blokhin B.M. Immersive simulation technologies for training practicing doctors in the skills of cardiopulmonary resuscitation for children/B.M. Blokhin, I.V. Gavryutina, V.Yu. Steshin, E.Yu. Ovcharenko, I.P. Lobushkova//Bulletin of the therapist 2018. № 7 (31). S. 4-11.

[7] Karelina M.V. Methodical aspects of the use of simulators with immersive technology when studying at the University of Transport/M.V. Karelin, S.P. Vakulenko, P.A. Egorov, O.V. Meretskov//Domestic and foreign pedagogy. 2021. VOL. 2. № 6 (81). S. 64-80.

[8] Yusupov A.A. Study of the human factor in training firefighters with immersion in virtual reality/ Yusupov A.A.//In the collection: Modern science: current issues, achievements and innovations. collection of articles of the XXIX International Scientific and Practical Conference. Penza, 2023. S. 260-262.

[9] Volkov S.D., Tsaregorodtsev A.V. One of the approaches to ensuring protection against computer attacks when implementing the information function of the state at the domestic level//Bulletin of the Perm National Research Polytechnic University. Electrical engineering, information technology, control systems. 2020. № 36. S. 159-174.

[10] Klimov S.M. Methods and models of countering computer attacks. Lyubertsy: CATALIT, 2008. SS. 64-64.

[11] Volkov S.D. Review of approaches to building computer attack detection systems for information and telecommunication systems operating on the basis of cloud computing technology//Collegium Linguisticum - 2017. Materials of the annual conference of the student scientific society of Moscow State Linguistic University. 2017. M.: FSBEI HE MSLU. S. 442-447.

[12] Stepashkin M.V., Kotenko I.V., Bogdanov V.S. Attack Modeling for Active Analysis of Computer Network Vulnerabilities//Second All-Russian Scientific and Practical Conference on Simulation Modeling and its Application in Science and Industry “Simulation Modeling. Theory and practice» IMMOD-2020. C. 269–273.