УДК 378.091.398
DOI: 10.26140/anip-2020-0903-0043

ИСПОЛЬЗОВАНИЕ ИННОВАЦИОННЫХ МЕТОДОВ И СОВРЕМЕННЫХ ТЕХНОЛОГИЙ ДЛЯ ПОВЫШЕНИЯ КВАЛИФИКАЦИИ В ОБЛАСТИ КИБЕРБЕЗОПАСНОСТИ

SPIN: 1713-3530
AuthorID: 732054
ORCID: 0000-0002-1202-4830

Нечай Александр Анатольевич, аспирант
Ленинградский государственный университет имени А.С. Пушкина
(196605, Россия, Санкт-Петербург, Петербургское шоссе, дом 10, e-mail: webexpromt@mail.ru)

Аннотация. Активное внедрение информационных технологий и компьютеризация всех сфер жизнедеятельности человека привело к необходимости развития такого направления как кибербезопасность. Помимо этого появилась необходимость разработки специализированного программного обеспечения для повышения квалификации и формированию у будущих педагогов навыков и умений грамотного поведения в киберпространстве. Анализ инцидентов связанных с киберугрозами свидетельствует о том, что проблема подготовки будущих учителей информатики к обучению школьников основам кибербезопасности выходит на первый план. Статья посвящена описанию возможных способов применения современных методов и технологий для повышения квалификации в области кибербезопасности. В статье представлены инновационные технологии, такие как электронное обучение, с использованием виртуальной и дополненной реальности повышающие интерес к обучению кибербезопасности. Электронное обучение с использованием технологий виртуальной и дополненной реальности позволяет проникнуть глубоко внутрь исследуемой проблемы, оказаться в эпицентре кибератаки и увидеть, как реализуется тот или иной инцидент нарушения безопасности. Электронные виртуальные технологии также позволяют в игровой форме отрабатывать и закреплять на практике действия по предотвращению кибератак, получать опыт в области кибербезопасности и повышать свою компетенцию. Автор статьи считает, что предложенный подход обучения кибербезопасности существенно повысит эффективность образовательного процесса и интерес к повышению квалификации среди действующих учителей и преподавателей информатики.

Ключевые слова: современные технологии, кибербезопасность, киберугроза, кибератака, электронное обучение, виртуальная реальность, дополненная реальность, повышение квалификации, инновационные технологии, компьютеризация, информатика, программное обеспечение, инновационные методы.

USE OF INNOVATIVE METHODS AND MODERN TECHNOLOGIES FOR ADVANCED TRAINING IN CYBERSECURITY

Nechai Alexander Anatolievich, postgraduate student
Leningrad State University named after A. S. Pushkin
(196605, Russia, Saint Petersburg, Peterburgskoe shosse 10, e-mail: webexpromt@mail.ru)

Abstract. The active introduction of information technologies and computerization of all spheres of human life has led to the need to develop such areas as cybersecurity. In addition, there is a need to develop specialized software for professional development and the formation of future teachers ‘ skills and abilities of competent behavior in cyberspace. Analysis of incidents related to cyber threats shows that the problem of preparing future computer science teachers to teach students the basics of cybersecurity comes to the fore. The article describes possible ways to apply modern methods and technologies to improve skills in the field of cybersecurity. The article presents innovative technologies, such as e-learning, using virtual and augmented reality that increase interest in cybersecurity training. E-learning using virtual and augmented reality technologies allows you to get deep inside the problem under study, find yourself in the epicenter of a cyber attack and see how a particular security incident is implemented. Electronic virtual technologies also allow you to practice and practice actions to prevent cyber attacks, gain experience in the field of cybersecurity and improve your competence. The author of the article believes that the proposed approach to cybersecurity training will significantly increase the effectiveness of the educational process and interest in professional development among current teachers and teachers of computer science.

Keywords: modern technologies, cyber security , cyber threat , cyber attack , e- learning, virtual reality, augmented reality, professional development, innovative technologies, computerization, computer science, software, innovative methods.

ВВЕДЕНИЕ

Информационный прогресс и повсеместная компьютеризация несет в себе угрозы связанные с киберпреступностью [1,2]. Вопросы кибербезопасности в настоящее время выходят на передний план [3,4].

Для того чтобы успешно противостоять кибератакам [5] требуются соответствующие специалисты которых до недавнего времени готовили только в ведомственных государственных учреждениях. В настоящее время обучение основам кибербезопасности начинают вводить на уроках информатики в образовательных организациях.

В связи, с чем встает вопрос как за короткий срок повысить квалификацию и компетентность учителей информатики в области кибербезопасности без существенного отрыва учителей от образовательного процесса, а так же сделать образовательный процесс более наглядным и интересным.

В настоящее время образовательные организации ведущие подготовку специалистов в области кибербезопасности в своей образовательной среде [6] стремятся использовать инновационные технологии, применяют интегративное обучение сочетающие традиционное аудиторное обучение с электронным обучением, чтобы повысить интерес у учителей и преподавателей информатики к повышению квалификации и приобретению компетенций в данной области.

Анализ научных работ посвященных повышению квалификации учителей и педагогических кадров показывает эффективность применения инновационных технологий в образовательном процессе. Федорова Г.А. [7] в своей научной статье рассматривает применение интерактивных технологий при подготовке учителей информатики и показывает их эффективность.

Подготовке будущих учителей информатики и математики к обучению школьников основам кибербезопасности посвящена совместная статья Троицкой О.Н. и Вохтомина Е.Д. [8], авторы рассматривают современные методы обучения и структурируют последовательность тех знаний и навыков, которыми должен обладать современный учитель.

В своем научном исследовании авторы Бороненко Т.А. и Федотова В.С. [9] рассматривают проблему формирования цифровой компетентности бедующих

учителей информатики, проводят сравнительный анализ инновационных технологий влияющих на формирование компетенции учителя информатики, рассматривают вопросы обучения учителей информационной безопасности и кибербезопасности.

Авторы рассмотренных работ делают акцент в своих работах на техническую составляющую повышения квалификации учителей, но помимо этого есть еще и эмоциональная составляющая, мотивирующая к обучению, которая повысит эффективность образовательного процесса и интерес к повышению квалификации среди действующих учителей и преподавателей информатики. Данная составляющая образовательного процесса интегрирована в инновационные технологии электронного обучения с использованием виртуальной [10] и дополненной реальности.

МЕТОДОЛОГИЯ

Целью статьи является рассмотрение таких инновационных методов и современных технологий для повышения квалификации в области кибербезопасности, которые бы позволили повысить эффективность и наглядность образовательного процесса, а также поддерживали высокую мотивацию к обучению.

Для достижения поставленной цели было проведено исследование применимости к обучению кибербезопасности электронного обучения включающего в себя технологию виртуальной реальности и технологию дополненной реальности.

РЕЗУЛЬТАТЫ

Электронное обучение [11] - это использование телекоммуникационных технологий [12] предоставления информации для целей образования и профессиональной подготовки. С развитием информационно-коммуникационных технологий электронное обучение становится одной из парадигм современного образования. Большие преимущества электронного обучения включают в себя освобождение взаимодействия между учащимися и преподавателями от ограничений времени и пространства с помощью асинхронной и синхронной модели сети обучения [13].

Электронное обучение обычно называют преднамеренным использованием сетевых информационно-коммуникационных технологий в преподавании и обучении. Для описания этого способа преподавания и обучения также используется ряд других терминов. Они включают в себя онлайн-обучение, виртуальное обучение, распределенное обучение, сетевое и веб-обучение. Термин «электронное обучение» включает в себя гораздо больше, чем онлайн-обучение [14], поскольку буква «E» в электронном обучении означает слово «электронный», электронное обучение будет включать в себя всю образовательную деятельность, осуществляемую отдельными лицами или группами.

Электронное обучение лучше всего можно определить как науку об обучении без использования бумажных печатных учебных материалов.

Рассмотрим применение электронного обучения кибербезопасности с использованием дополненной и виртуальной реальности.

Бурное развитие технологий виртуальной и дополненной реальности может обеспечить обучение в области кибербезопасности новыми идеями, инновационными решениями и практическим опытом. Основными преимуществами интеграции таких технологий [15] в учебный процесс являются: более быстрое обучение за счет эффективности передачи навыков, приобретение и оценка знаний в реальном времени, безопасность практики, более активное вовлечение за счет использования внеклассовой учебной среды и возможность практического обучения.

Виртуальная реальность это компьютерная симуляция реальной среды, которая с помощью стимуляции зрения и слуха заставляет пользователя чувствовать себя так, как будто он сам переживает моделируемую реальность.

Технологии дополненной реальности предоставляют своим пользователям представление о физической, реальной среде, элементы которой дополняются компьютерным вводом, таким как видео, графика или звук. Будучи похожими, виртуальная и дополненная реальность отличаются тем, что виртуальная реальность в цифровом виде воссоздает реальную обстановку, в то время как дополненная реальность использует цифровые элементы в качестве наложения на реальный мир. Используя технологии виртуальной и дополненной реальности при обучении кибербезопасности можно выделить три основных положительных эффекта: обучающие могут на себе испытать последствия допущенных ошибок, обучение строится в виде игры и наблюдается повышенный интерес и вовлеченность в образовательный процесс.

Одним из главных преимуществ технологий виртуальной и дополненной реальности [16] является то, что обучающиеся кибербезопасности могут испытать на себе виртуальные последствия своих ошибок. Например, если обучающийся не может идентифицировать виртуальное вложение, содержащее программу-вымогатель, он может наблюдать за виртуальными последствиями программы-вымогателя, такими как шифрование файлов и отображение сообщения с просьбой о выплате выкупа.

В контексте обучения кибербезопасности такие технологии могут использоваться для предоставления инструкций обучаемым во время моделирования инцидентов. Например, технологии виртуальной и дополненной реальности могут предоставить учителю, который проводит обучение по кибербезопасности, инструкции о том, как проинструктировать каждого обучающегося о шагах, направленных на снижение воздействия кибератаки.

Поскольку технологии виртуальной и дополненной реальности могут распознавать объекты, такие технологии могут быть использованы для обучения тому, как выявлять лазейки безопасности в реальной среде, такие как слабые пароли, публикация информации, которая может быть использована для проведения кибератак, фишинговые письма, отсутствие антивирусного программного обеспечения и вредоносные веб-сайты.

Технологии виртуальной и дополненной реальности [17] также могут быть использованы для геймификации обучения кибербезопасности. Электронное обучение на основе игр приносит множество преимуществ, таких как вызов, мотивация и привлечение аудитории, а также изучение последствий в безопасной виртуальной среде.

Например, обучающихся виртуальной игры можно разделить на две команды, а именно на нападающих киберпреступников и защитников, специалистов отвечающих за кибербезопасность.

Злоумышленники могут получать баллы за выявление уязвимостей информационной безопасности, склонение жертв к открытию вредоносных вложений и проведение успешных кибератак. Защитники могут получать баллы за выявление киберугроз, реализацию соответствующих стратегий кибербезопасности, информирование об инцидентах кибербезопасности и соблюдение политики безопасности.

Таким образом, получая баллы и виртуальные знаки отличия, обе команды будут приобретать практические навыки кибербезопасности в эмоционально привлекательной форме. Эмоциональная вовлеченность в игровой образовательный процесс очень хорошо стимулирует участников образовательного процесса, позволяет более эффективно усваивать те навыки, которые они получили.

Учебные занятия, реализуемые с помощью технологий виртуальной и дополненной реальности, требуют от участников активного участия в образовательном про-

цессе.

Такое участие приводит к более высокому уровню вовлеченности в образовательный процесс.

Учебные материалы, реализуемые посредством технологий виртуальной и дополненной реальности, благодаря их высокому визуальному и эмоциональному воздействию направленные на повышение осведомленности в кибербезопасности эффективно могут быть применены для обучения среди различных возрастных групп людей.

Технологии виртуальной реальности могут использоваться, по меньшей мере, в трех типах обучающих приложений по кибербезопасности, а именно: в приложениях, позволяющих обучающимся видеть примеры информационной инфраструктуры, в приложениях, позволяющих реагировать на кибератаки и в приложениях, предоставляющих инструкции о том, как проводить различные профилактические мероприятия, связанные с кибербезопасностью.

Приложения, использующие технологии виртуальной и дополненной реальности [18, 19] позволяют изучать различные типы информационной инфраструктуры, например информационную инфраструктуру атомных станций, аэропортов и железных дорог. Например, технологии виртуальной реальности могут быть использованы для изучения промышленных компьютерных систем, атакованных вредоносным компьютерным червем Stuxnet [20]. Stuxnet - это чрезвычайно сложный компьютерный червь, который использует множество ранее неизвестных уязвимостей нулевого операционной системы Windows для заражения компьютеров и распространения. Его цель состояла не только в том, чтобы заразить компьютеры, но и вызвать реальные физические эффекты. В частности, он нацелен на центрифуги, используемые для производства обогащенного урана, который приводит в действие ядерное оружие и реакторы. Stuxnet нанес существенный ущерб Иранским ядерным объектам [21].

Приложения, использующие технологии виртуальной и дополненной реальности так же позволяют непосредственно переместиться в центр кибератаки, увидеть, как она реализована, что позволит обучающимся развивать свои навыки реагирования на инциденты, а также навыки совместной работы в команде. Этот тип электронного обучения гарантирует, что обучающие будут погружены в реалистичные инцидентные ситуации, не испытывая эмоциональных и когнитивных эффектов, связанных с реальной опасностью.

Технологии виртуальной реальности могут быть использованы для предоставления инструкций о том, как выполнять различные мероприятия, связанные с кибербезопасностью в реалистичной среде. Повторяя их многократно, обучающиеся таких технологий смогут запоминать и применять их в реальных жизненных ситуациях.

ВЫВОДЫ

Применение современных методов и технологий в обучении и повышении квалификации в области кибербезопасности является оправданным.

Инновационные технологии, такие как электронное обучение, с использованием виртуальной и дополненной реальности повышают интерес к обучению, позволяют проникнуть глубоко внутрь исследуемой проблемы, оказаться в эпицентре кибератаки и увидеть, как реализуется тот или иной инцидент нарушения безопасности.

Электронные виртуальные технологии также позволяют в игровой форме отрабатывать и закреплять на практике действия по предотвращению кибератак, получать опыт в области кибербезопасности и повышать свою компетенцию.

СПИСОК ЛИТЕРАТУРЫ:

1. Ефремов М.А., Казаманова К.М., Ширяева А.В. Актуальные вопросы кибербезопасности, и повышения финансовой грамотности в эпоху цифровых технологий // Международная конференция по мягким вычислениям и измерениям. 2019. Т. 1. С. 402-405.

2. Векшарева Д.М. Человек IT-цивилизация. крупнейшие кибератаки // В сборнике: Россия и мир в новое и новейшее время - из прошлого в будущее материалы XXV юбилейной ежегодной международной научной конференции: в 4 т.. 2019. С. 101-102.

3. Нечай А.А., Котиков П.Е. Методика комплексной защиты данных, передаваемых и хранимых на различных носителях информации // Вестник Российского нового университета. Серия: Сложные системы: модели, анализ и управление. 2015. № 1. С. 92-95.

4. Котиков П.Е., Нечай А.А. Решение проблемы управления параллельным выполнением транзакций в распределенных базах данных для устранения опасной противоречивости // Вестник Российского нового университета. Серия: Сложные системы: модели, анализ и управление. 2015. № 2. С. 62-64.

5. Нечай А.А., Котиков П.Е. Актуальные проблемы защиты информации в современных автоматических телефонных станциях Вестник Российского нового университета. Серия: Сложные системы: модели, анализ и управление. 2015. № 2. С. 65-69.

6. Нечай А.А. Формирование безопасной информационной среды // Актуальные проблемы современности: наука и общество. 2019. № 4 (25). С. 43-44.

7. Федорова Г.А. Интерактивные технологии в методической подготовке будущих учителей информатики // В книге: Дистанционное обучение в высшем образовании: опыт, проблемы и перспективы развития 2019. С. 28-30.

8. Трощкая О.Н., Вохтомина Е.Д Подготовка будущих учителей математики и информатики к обучению школьников основам кибербезопасности // Информатика и образование. 2019. № 8 (307). С. 24-31.

9. Бороненко Т.А., Федотова В.С. Проблема формирования цифровой компетентности будущего учителя информатики в условиях цифровизации российской школы // В сборнике: Подготовка педагогов в контексте инновационных изменений в высшем образовании Сборник статей научно-практической конференции. Редакционный совет: А.П. Тряпицына , Н.В. Примчук. 2019. С. 183-189.

10. Саидов Ж.А., Жулибекова Ф.А. Причины использования виртуальной реальности в образовательных и обучающих курсах, и модель определяющая, когда использовать виртуальную реальность // В сборнике: Студенческие научные достижения сборник статей VI Международного научно-исследовательского конкурса. 2019. С. 30-35.

11. Корбут К.Э. Электронное обучение или машинное обучение: четвёртая научно-техническая революция - прогресс или вызов человечеству? // В сборнике: Интеллектуальный потенциал образовательной организации и социально-экономическое развитие региона. Сборник материалов международной научно-практической конференции Академии МУБиНТ. Образовательная организация высшего образования (частное учреждение) «Международная академия бизнеса и новых технологий (МУБиНТ)». 2019. С. 176-178.

12. Коростелева Н.А., Лукичева Н.М. Об использовании обучающих информационных сред в эпоху цифровой экономики // В сборнике: Инновационные доминанты социально-трудовой сферы: экономика и управление Материалы ежегодной международной научно-практической конференции по проблемам социально-трудовых отношений. Редакционная коллегия: А.А. Федченко, О.А. Колесникова. 2019. С. 134-137.

13. Курсевич Д.В. Адаптивная модель развития профессионально-коммуникативной компетентности будущих специалистов в сферах информационных технологий и кибернетики // Муниципальное образование: инновации и эксперимент. 2019. № 6 (69). С. 13-17.

14. Александрова А.А., Вяхирева М.А., Сердюк А.А. Особенности образования с использованием онлайн обучения // В сборнике: Сборник трудов научно-практической и учебной конференции. 2019. С. 3-7.

15. Романов А.А., Лунькова Е.Ю. Потенциал информационно-образовательной среды университета в обучении будущих педагогов // В сборнике: Образовательное пространство в информационную эпоху - 2019 Сборник научных трудов. Материалы Международной научно-практической конференции. Под редакцией С.В. Ивановой. 2019. С. 631-645.

16. Кулумбегов Ян.М., Зуккель Е.Д., Коробейникова Е.В. Использование технологий виртуальной и дополненной реальности в образовании и других сферах деятельности // В сборнике: Инновационный конвент «Кузбасс: образование, наука, инновации» Материалы Инновационного конвента. Департамент молодежной политики и спорта Кемеровской области. 2019. С. 570-571.

17. Набокова Л.С., Загидуллина Ф.Р. Перспективы внедрения технологий дополненной и виртуальной реальности в сферу образовательного процесса высшей школы // Профессиональное образование в современном мире. 2019. Т. 9. № 2. С. 2710-2719.

18. Астафьев А.О., Гущина О.М. Приложения дополненной реальности, опыт разработки // В сборнике: Информационные технологии в моделировании и управлении: подходы, методы, решения Сборник научных статей II Всероссийской научной конференции с международным участием. В 2 частях. 2019. С. 416-421.

19. Жигалова О.П., Толстопятов А.В. Использование технологии дополненной реальности в образовательной сфере // Балтийский гуманитарный журнал. 2019. Т. 8. № 2 (27). С. 43-46.

20. Анализ проблем безопасности автоматизированых систем управления технологическими процессами Бабкин А.Ю. В сборнике: Инжиниринг предприятий и управление знаниями (ИП&УЗ-2019) Сборник научных трудов XXII Международной научной конференции. В 3-х томах. Под научной редакцией Ю.Ф. Тельнова.

2019. С. 31-35.

21. Остроцкая С.В., Калуцкий И.В. К вопросу анализа угроз безопасности критическим информационным инфраструктурам // В сборнике: Информационные технологии в моделировании и управлении: подходы, методы, решения Материалы II Всероссийской научной конференции с международным участием. В 2 частях. 2019. С. 212-217.

Статья поступила в редакцию 19.03.2020
Статья принята к публикации 27.08.2020