Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Южно-Уральский государственный гуманитарно-педагогический университет»
(ФГБОУ ВО «ЮУрГГПУ»)

Факультет дошкольного образования

Кафедра педагогики и психологии детства

ИНФОРМАЦИОННАЯ КУЛЬТУРА СОВРЕМЕННОГО ДЕТСТВА

Сборник статей
Международной научно-практической конференции

Россия, г. Челябинск,
31 октября — 1 ноября 2019 года

Челябинск ● 2019

УДК 004.8-053
ББК 71.0
И74

Информационная культура современного детства [Текст] : сборник
И74 статей Международной научно-практической конференции «Информационная культура современного детства» (г. Челябинск, 31 октября — 1 ноября 2019 года). – Челябинск : Издательский центр «Титул», 2019. – 250 с.

ISBN 978-5-6043555-4-1

В сборнике представлены научно-методические статьи педагогов, студентов, магистрантов, аспирантов России, Китая, Узбекистана, Белоруссии, подводящие промежуточные итоги научных изысканий по проблеме формирования информационной культуры современного детства. В материалах статей отражена практическая реализация идей формирования информационной культуры современных детей в образовательном пространстве. Результаты проведенных исследований способствуют определению дальнейших перспектив решения задач дошкольного и начального общего, профессионального образования с учетом социального заказа и требований федеральных государственных образовательных стандартов.

Сборник научно-методических статей адресован педагогическим работникам различных уровней образования: руководителям дошкольных и общеобразовательных организаций, педагогам дошкольного образования, учителям общеобразовательных организаций, студентам и преподавателям педагогических университетов и педагогических колледжей.

УДК 004.8-053
ББК 71.0

Сборник издан при финансовой поддержке гранта РФФИ № 18-013-00743 А «Становление основ информационной грамотности дошкольников».

ISBN 978-5-6043555-4-1

2. Горюнова М.А., Семенова Т.В., Солоневичева М.Н. Интерактивные доски и их использование в учебном процессе: Информатика и информационно-коммуникационные технологии // СПб.: БХВ-Петербург, 2010. 336 с.: ил. + CD-ROM.
3. Гребенюк Е.И., Гребенюк Н.А. Технические средства информатизации: учебник для студ. сред. проф. образования. 3-е изд., стер. М.: Издательский центр Академия, 2007. 272 с.
4. Иванова И.И. Методические рекомендации по использованию интерактивной доски в учебном процессе /под ред. Ганичевой Е.М.; Департамент образования Вологод. обл., Вологод. ин-т развития образования. Вологда: ВИРО, 2012. 32 с.
5. Калитин С.В. Интерактивная доска. Практика эффективного применения в школах, колледжах и вузах: Элективный курс. Профильное обучение. М.: Солон-Пресс, 2013. 192 с.

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ЭЛЕКТРОННОМ ОБУЧЕНИИ

Э.Р. Галиуллина, Р.С. Зарипова
Россия, г. Казань, КГЭУ
zarim@rambler.ru

Аннотация: В данной статье приведен обзор наиболее важных проблем кибербезопасности, имеющих отношение к системам высшего образования и будущим распределенным системам электронного обучения. Охвачены основные разделы: кибербезопасность и образование; угрозы безопасности, обнаружение и защита в распределенных системах электронного обучения; разработка модели управления безопасностью для систем электронного обучения.

Abstract: This paper gives an overview of the most important cybersecurity issues related to higher education systems and future distributed e-learning systems. The main sections are covered: cybersecurity and education; security threats, detection and protection in distributed e-learning systems; developing a security management model for e-learning systems.

Ключевые слова: электронное обучение, высшее учебное заведение, кибербезопасность, электронные системы, информация.

Keywords: e-learning, higher education institution, cybersecurity, electronic systems, information.

Системы электронного обучения являются сложными системами, направленными на обеспечение потребностей учащихся и поддержку хорошего имиджа учебного процесса [1]. Имеются четкие доказательства того, что инновационные образовательные технологии, такие как электронное обучение, предоставляют беспрецедентные возможности для студентов, слушателей и преподавателей получать, развивать и поддерживать основные навыки и знания [2]. Однако системы электронного обучения используют Интернет как место для получения всей необходимой информации и знаний. К сожалению, Интернет также стал местом проведения новомодной незаконной деятельности, так называемой киберпреступности [3]. Информация, связанная с электронной средой обучения, часть которой может носить личный, защищенный или конфиденциальный характер, постоянно подвергающаяся угрозами

безопасности, поскольку системы электронного обучения являются открытыми, распределенными и взаимосвязанными.

За последние годы электронное обучение получило впечатляющее развитие. Системы электронного обучения разнообразны и широко распространены, например, WebCT, Moodle и Blackboard. Они большие и динамичные с различными пользовательскими надстройками и ресурсами. Обмен информацией, сотрудничество и взаимодействие являются основными элементами любой системы электронного обучения. Из этого следует, что все данные должны быть защищены для обеспечения конфиденциальности, целостности и доступности. Защита от манипулирования данными, мошеннической аутентификации пользователей и компромиссов в конфиденциальности является важным вопросом безопасности в электронном обучении. В то же время тенденции в области электронного обучения требуют повышения уровня совместимости приложений, учебных сред и гетерогенных систем.

Системы электронного обучения имеют те же характеристики и проблемы, что и другие электронные услуги, требующие обмена и распространения информации. Более конкретно они связаны с доступностью услуг через Интернет, потреблением услуг человеком через Интернет и оплатой услуг клиентом [4]. Организации должны уделять больше внимания управлению рисками безопасности, принимая во внимание тип и серьезность различных угроз и уязвимостей, а также признавая разнообразное взаимодействие и интеграцию между клиентами, серверами, базами данных и другими компонентами.

Электронные системы уязвимы перед рядом угроз: серьезные угрозы безопасности включают программные атаки (вирусы, черви, макросы, отказ в обслуживании), шпионаж, акты кражи (незаконное оборудование или информация) и интеллектуальная собственность (пиратство, нарушение авторских прав). Системы электронного обучения имеют некоторые особенности, имея множество пользователей, множество приложений и информации для загрузки и выгрузки.

Электронные системы уязвимы для целого ряда угроз безопасности:

- аутентификация – нарушенная аутентификация и управление сеансами;
- доступность – отказ в обслуживании;
- конфиденциальность – небезопасное криптографическое хранилище; небезопасная прямая ссылка на объект; утечка информации;
- целостность – переполнение буфера; подделка межсайтовых запросов; межсайтовый скриптинг; невозможность ограничить доступ к URL.

Угроза определяется как категория объекта, человека или других объектов, представляющих опасность, таких как трояны или фишинг. Схемы, включающие аутентификацию пользователей на основе паролей, очень чувствительны к фишинговым атакам, которые становятся все более изощренными и требуют решительных профилактических и контрмер.

Высшие учебные заведения должны применять корпоративные подходы к управлению рисками информационной безопасности в рамках существующих

структур управления [5]. Учреждения должны идентифицировать «контроли» данных, чтобы установить четкие линии информации в учреждении, которое безопасно распространяет информацию в распределенной среде.

Реализация управления кибербезопасностью требует соответствующего уровня понимания угроз, стоящих перед университетом, и мер, которые были приняты. Это потребует повседневной ответственности за надлежащую оценку, управление и отчетность по рискам. Руководители учреждений, весь академический персонал и ИТ-группа в высшем учебном заведении должны быть в курсе информации об их обязанностях и предупреждать о возникающих угрозах и рисках для пользователей данных [6].

Все высшие учебные заведения должны осознавать свои обязанности в отношении защиты институциональных и исследовательских данных и иметь соответствующие меры для обеспечения их соответствия Федеральному закону «О персональных данных» (2006 г.). Большинство высших учебных заведений будут иметь различные структуры для управления данными и исследованиями, а также соответствующие уровни контроля [7]. У большинства из этих учреждений и исследователей будет различная политика и планы по управлению данными, и при этом очень мало будет проблем с ошибками. Эти функции представляют собой проблему для корпоративного управления, чтобы понять, как проблемы, так и необходимость модели процессов угроз и кибербезопасности сотрудников.

В конце концов, безопасность сети – это ответственность всего учреждения. Сетевые администраторы могут постоянно получать информацию об угрозах и мерах противодействия путем обмена информацией с коллегами и другими руководствующими структурами. Более важны пользователи, для которых они имеют решающее значение для безопасности любой сети и информации. Они должны играть центральную роль в оценке риска, с которым сталкиваются информация, приоритеты безопасности и, наконец, как пользователи, они несут ответственность за реализацию мер контроля.

Потребность в электронном обучении изменила способ, которым высшее образование ведет повседневную деятельность, проявляя все большую активность в создании или поиске новых услуг, которые могут позволить студентам учиться в виртуальной среде [8]. Повышенная потребность в мобильности и расширении возможностей электронного обучения представляет собой серьезную проблему для ИТ-отделов высшего образования, которым все труднее поддерживать контроль над тем, как данные используются, хранятся и совместно используются внутри и за пределами стен университета [9]. Понимание потребностей пользователей и внедрение новых услуг требует создания безопасных, стандартизированных, высокодоступных сред электронного обучения, а также централизованного управления приложениями.

Литература

1. Зарипова Р.С., Пырнова О.А. Особенности и тенденции развития современного инженерного образования / Современные исследования социальных проблем. Красноярск: Научно-Инновационный Центр, 2018. Т. 9. № 8-2. С. 43-46.

2. Шакиров А.А., Зарипова Р.С. Технологии больших данных в области информационной безопасности / International Journal of Advanced Studies in Computer Engineering. 2018. № 2. С. 74-77.

3. Зарипова Р.С., Г.Р. Залялова Современные тенденции подготовки инженеров / Нефтегазовый комплекс: проблемы и инновации: Тезисы II научно-практической конференции с международным участием. Самарский государственный технический университет. 2017. С. 42.

4. Пырнова О.А., Зарипова Р.С. Интернет как средство обучения / International Journal of Advanced Studies in Education and Sociology. 2018. № 2. С. 41-44.

5. Злыгостев Д.Д., Зарипова Р.С. Информационная безопасность как инструмент обеспечения экономической безопасности предприятий / Инновации в информационных технологиях, машиностроении и автотранспорте. Кемерово, 2017. С. 23-25.

6. Шакиров А.А., Зарипова Р.С Актуальность обеспечения информационной безопасности в условиях цифровой экономики / Инновационное развитие экономики. Будущее России. 2018. С. 257-260.

7. Зарипова Р.С., Пырнова О.А. Особенности и тенденции развития современного инженерного образования / Современные исследования социальных проблем. Красноярск: Научно-Инновационный Центр, 2018. Т.9. № 8-2. С.43-46.

8. Ширмамедова З.Н., Зарипова Р.С. Роль открытых электронных образовательных ресурсов в современном информационно-образовательном пространстве / Учёные записки ИСГЗ. 2019. Т.17. № 1. С.536-539.

9. Кривоногова А.Е., Зарипова Р.С. Современные информационные технологии и их применение в сфере образования / Russian Journal of Education and Psychology. 2019. Т. 10. № 5. С. 44-47.

К ВОПРОСУ О МЕТОДИЧЕСКОМ СОПРОВОЖДЕНИИ ПЕДАГОГОВ ДОО К ПРОЦЕДУРЕ АТТЕСТАЦИИ СРЕДСТВАМИ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

В.А. Горбунова, С.М. Зырянова
Россия, г. Сургут, БУ ВО «СурГПУ»
leri-89@mail.ru, zyryanova-zsm@yandex.ru

Аннотация: статья посвящена проблеме подготовки педагогических работников к процедуре аттестации, применению новых форм методической работы в межаттестационный период на основе информационно-коммуникационных технологий. В результате научного исследования (изучение психолого-педагогической литературы по изучаемой проблеме, анализ нормативно-правовой документации, анкетирование) получены данные, свидетельствующие о необходимости внедрения в методическую деятельность инновационных технологий в работе с педагогическими работниками по вопросам прохождения процедуры аттестации. Предлагаемые авторами практические материалы рекомендованы к использованию в деятельности дошкольных образовательных организаций как в процессе подготовки педагогов к процедуре аттестации, так и в практическом применении в рамках организации всего образовательного процесса в ДОО.

Abstract: the article is devoted to the problem of training of teachers to the certification procedure, the use of new forms of methodical work in the inter-certification period on the basis of information and communication technologies. As a result of scientific research: questioning, studying of psychological and pedagogical literature on the studied problem, and also the analysis of normative and legal documentation. The data indicate the need for the introduction of methodological activities of innovative technologies in working with teachers on the passage of the