УДК 004: 378

Казанский государственный энергетический университет
Студентка Э.Р. Галиуллина
Канд. техн. наук, доцент Р.С. Зарипова,
Россия, г. Казань
E-mail: zarim@rambler.ru

Kazan State Power Engineering University
Student E.R. Galiullina
Cand. tech. Sci., Assoc. R.S. Zaripova,
Russia, Kazan
E-mail: zarim@rambler.ru

Э.Р. Галиуллина, Р.С. Зарипова

ПРОБЛЕМЫ КИБЕРБЕЗОПАСНОСТИ ДЛЯ ВИРТУАЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ СРЕДЫ

Аннотация: В данной работе дается 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; и представлены некоторые выводы.

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

E.R. Galiullina, R.S. Zaripova

CYBER SECURITY PROBLEMS FOR VIRTUAL EDUCATIONAL ENVIRONMENT

Annotation: 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; development of a security management model for e-learning systems; and some conclusions are presented.

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

Системы электронного обучения являются сложными системами, направленными на обеспечение потребностей учащихся и поддерживать хороший имидж учебного процесса. 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 [1]. 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. 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 [2]. 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. 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 интеллектуальную 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 [3]. 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.

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). Большинство высших учебных заведений будут иметь различные структуры для управления данными и исследованиями, а также соответствующие уровни контроля. 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 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. 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. Понимание потребностей пользователей и внедрение новых услуг требует создания безопасных, стандартизированных, высокодоступных сред электронного обучения, а также централизованного управления приложениями.

Библиографический список

1. Зарипова Р.С. Особенности и тенденции развития современного инженерного образования / Р.С. Зарипова, О.А. Пырнова / Современные исследования социальных проблем. – Красноярск: Научно-Инновационный Центр, 2018. – Т.9. – №8-2. – С.43-46.
2. Кривоногова А.Е. Современные информационные технологии и их применение в сфере образования / А.Е. Кривоногова, Р.С. Зарипова / Russian Journal of Education and Psychology. – 2019. –Т. 10. – №5. – С. 44-47.
3. Ширмамедова З.Н. Роль открытых электронных образовательных ресурсов в современном информационно-образовательном пространстве / З.Н. Ширмамедова, Р.С. Зарипова / Учёные записки ИСГЗ. – 2019. – Т.17. – №1. – С.536-539.
4. Галиуллина Э.Р. Образовательные цифровые игры как способ обучения студентов / Э.Р. Галиуллина, Р.С. Зарипова / International Journal of Advanced Studies in Education and Sociology. – 2019. – № 1. – С. 9-13.
5. Шакиров А.А. Технологии больших данных в области информационной безопасности / А.А. Шакиров, Р.С. Зарипова / International Journal of Advanced Studies in Computer Engineering. – 2018. – № 2. – С. 74-77.
6. Пырнова О.А. Интернет как средство обучения / О.А. Пырнова, Р.С. Зарипова / International Journal of Advanced Studies in Education and Sociology. – 2018. – № 2. – С. 41-44.