МЕТОДЫ ПОВЫШЕНИЯ ЗАЩИЩЁННОСТИ ТЕСТОВЫХ ОБУЧАЮЩИХ СИСТЕМ

Кравцова Л.В., Каминская Н.Г.
Херсонская государственная морская академия (Украина)

В 2015-2016 учебном году в ХГМА начала своё существование система дистанционного обучения, созданная на базе платформы Moodle (Modular Object-Oriented Dynamic Learning Environment — модульная объектно-ориентированная динамическая обучающая среда), предназначенной для объединения педагогов, администраторов и обучающихся (учеников, студентов) в одну надёжную, безопасную, интегрированную систему для создания персонализированной обучающей среды [1]. Проект СДО Moodle ХГМА разработан и внедрён в учебный процесс коллективом кафедры информационных технологий, компьютерных систем и сетей академии. При этом было необходимо обеспечить качественную поддержку учебного процесса (смешанное обучение), проведение комплексной проверки знаний, профессиональных умений и навыков в режиме независимого компьютерного тестирования с учётом специфики подготовки моряка международного уровня. В 2016-2017 учебном году руководством академии было принято решение о проведении независимого экзаменационного тестирования по всем дисциплинам, формой контроля знаний по которым был экзамен. Для объективной оценки знаний курсанта по каждой дисциплине на сайте дистанционного обучения был сформирован банк тестовых вопросов, покрывающих весь учебный материал дисциплины. Система автоматически формирует для каждого тестируемого персональный вариант, учитывающий типы заданий, уровень сложности, тематику, время, отведённое на тестирование. Естественно, подготавливает тест и отвечает за его качество преподаватель дисциплины. С другой стороны, руководитель проекта, администратор сайта дистанционного обучения, учебный отдел должны обеспечить объективность проверки знаний в тестовом режиме.

К обучающим системам, в том числе и Moodle, используемой в ХГМА, предъявляются высокие требования, такие как защита от копирования, списывания и несанкционированного доступа к вопросам; наличие большой тестовой базы; простота программного интерфейса; удобство администрирования теста; полная автоматизация процесса тестирования; минимизация времени посылки запроса / получения отклика системы. В информационной безопасности существует понятие информационного риска, и это имеет прямое отношение к СДО Moodle ХГМА. Существуют различные способы защиты информации, в том числе и кардинальные. В рамках этого материала рассмотрим основные положения по защите информации, которые разработаны администрацией проекта и успешно применяются в использовании СДО в учебном процессе. Следует отметить, что доступ к электронным образовательным ресурсам СДО Moodle ХГМА предоставляется курсантам и студентам академии через процесс авторизации на портале https://mdl.ksma.ks.ua/ [2] с использованием индивидуального логина и пароля. Регистрация и/или удаление обучающихся в академии осуществляется администратором согласно приказам ректора академии о зачислении, распределении, переводе и восстановлении обучающегося. Доступ к ресурсам электронной информационно-образовательной среды ХГМА предоставляется после подписания соглашения о выполнении Правил использования ресурсов и ответственности пользователя. Приведём некоторые положения Правил. Веб-сервисы, базы данных и ресурсы элементов СДО Moodle ХГМА являются интеллектуальной собственностью Академии. Пользователи СДО имеют возможность доступа к персонализированной части электронной информационно-образовательной среды и обязаны использовать информацию с соблюдением авторских прав, не воспроизводить полностью или частично информацию ограниченного доступа. Пользователь, прошедший процедуру регистрации, в полной мере ответственен за сохранность регистрационных данных и обязуется нести ответственность за неумышленное или умышленное разглашение регистрационной информации, в результате собственной некомпетентности при работе с ресурсами и сервисами, в частности, за передачу своего логина и пароля другому лицу. Также пользователь несёт ответственность за умышленное использование программных средств (вирусов,

и/или самовоспроизводящегося кода), позволяющих осуществлять несанкционированное проникновение в электронные ресурсы с целью модификации информации, кражи паролей, угадывания паролей и других несанкционированных действий. Кроме того, пользователь обязуется соблюдать правила электронной этики внутри сетевого учебного сообщества ХГМА, а именно: компетентно отвечать в форумах, обсуждениях, опросах и других формах сетевого общения; проявлять корректность в общении с другими участниками сетевого сообщества.

Пользователь обязан немедленно уведомить администратора СДО ХДМА (непосредственно или через электронное сообщение) в случае невозможности авторизованного входа с первичным паролем, с целью временного блокирования доступа в систему от имени этого обучающегося, а также о любом нарушении безопасности. В случае потери учетных данных возможно восстановление доступа к учетной записи пользователя на СДО, для этого он должен непосредственно лично обратиться к администратору сайта для восстановления пароля. Администратор СДО Moodle ХГМА оставляет за собой право запретить использование определенных логинов (паролей) и/или изъять их из обращения.

Самая важная часть системы защиты информации на СДО ХДМА – это система разграничения доступа разных пользователей к различным таблицам. На сайте дистанционного обучения регистрируется большое количество пользователей. Каждый пользователь имеет свои права на каждую таблицу базы данных. Каждый из них может быть отнесён к определённой роли, и тогда права задаются только для нескольких ролей. Например, пользователь, являющийся студентом, не имеет права записывать данные в журнал с оценками. Но возможно, что кто-то из студентов захочет исправить себе плохую оценку в журнале и попытается взломать доступ к базе данных с помощью ввода SQL- команд в поля ввода интерфейсной части системы дистанционного обучения. Если в интерфейсе системы не реализована защита от подобных атак, то введённые злоумышленником SQL-команды выполнятся в СУБД. Причём, используя различные команды, можно не только исказить информацию в базе данных, но даже удалить сразу целую таблицу. Или можно прочитать некие засекреченные данные. Чтобы надёжно защитить базу данных от подобных атак, нужно использовать разграничение доступа. Различным пользователям (или пользователям различных ролей) нужно предоставить права доступа только на те таблицы, к которым им нужен доступ, и только доступ такого вида, который действительно нужен. Например, пользователь с правами студента имеет право читать данные из журнала оценок, но ни в коем случае не имеет права записывать какие либо данные в журнал. Кроме того, администратор следит за всеми действиями, которые пользователи совершают над базой данных. Например, это может понадобиться для того, чтобы определить, не были ли допущены ошибки при создании матрицы разграничения доступа. Для этого используется журнал аудита, в котором записываются все действия, совершаемые пользователями над базой данных. В журнале сохраняются имена пользователей, выполнивших действия, время, в которое каждое действие было выполнено, а также SQL-команды, которые были выполнены в каждом действии. Такие меры позволяют почти полностью исключить возможность несанкционированного доступа к информации, её искажения или уничтожения.

Выводы. Каждый ресурс в сети Интернет, в том числе и сайт дистанционного обучения ХДМА, должен быть снабжен грамотной системой безопасности. Практика показывает, что осознание всей важности этого действия приходит уже после того, как уязвимость обнаружена, сайт взломан, а информация украдена, изменена или уничтожена. Чтобы этого не произошло, необходимо заранее просчитать все риски для системы и максимально обезопасить её уже на стадии разработки.

ЛИТЕРАТУРА

1. Триус Ю.В. Система електронного ВНЗ на базі MOODLE: Методичний посібник / Ю. В. Триус, І. В. Герасименко, В. М. Франчук // За ред. Ю. В. Триуса. – Черкаси. – 2012. – 220 с.

2. Кравцов Г.М. Система моніторингу якості електронних інформаційних ресурсів вузу / Г.М.Кравцов // Інформаційні технології в освіті. - 2008. - № 2. - С. 42-46.

3. Кухаренко В.М. Системний підхід до змішаного навчання / В.М.Кухаренко // Інформаційні технології в освіті. - 2015. - № 24. - С. 53-67.