ОРГАНИЗАЦИЯ БЕЗОПАСНОСТИ В ОБУЧАЮЩИХ СИСТЕМАХ

А.В. Саскевич

При разработке информационных обучающих систем вопрос безопасности может оказаться вне зоны внимания разработчиков и исследователей. Тем не менее, обучающие системы, находящие свое применение в таких сферах как авиация, медицина, инженерия, требуют адекватного подхода к вопросу технической организации безопасности, так как это может повлиять как на подготовку учащихся, так и на их качество работы в будущем [1].

Разделение процесса организации безопасности позволяет разделить подходы, применяя их точечно в рамках задач, для которых они предназначены [2]. Информационная обучающая система подразумевает организацию безопасности как внешне – от несанкционированного доступа, DDoS-атак, так и изнутри – от попыток учащихся получить доступ, например, к ответам на тесты, или к редактированию итоговых оценок. Для внешней защиты подойдут классические методы и системы, такие как, например, фаервол. Для защиты изнутри могут применяться методы изоляции процессов в ОС, формирование уровней доступа пользователей и организация системы привилегий. В некоторых случаях информационные обучающие системы подразумевают возможность выполнения пользовательского кода. В данном случае потребуется изоляция исполняемого процесса, например, в виртуальную машину или контейнер.

Таким образом, при разработке обучающих систем необходимо обеспечить адекватный уровень изоляции пользователей, учебного и тестового материала, в ряде случаев обеспечить физическую и сетевую изоляцию машины, уровни доступов для учащихся разных направлений и категорий, а также, при разработке конкурирующей информационной системы, применить методики защиты информации и повышения отказоустойчивости системы.

Литература

1. Данилов А.Н., Шабуров А.С. О проблеме информационной безопасности открытых образовательных систем // Информационные войны. – 2013. – №. 1. – С. 89–95.

2. Загинайлов Ю.Н. Теория информационной безопасности и методология защиты информации. – Directmedia, 2015.