УДК 004.89

Г.В. РЫБИНА, А.Ю. НИКИФОРОВ, А.А. ГРИГОРЬЕВ

*Национальный исследовательский ядерный университет «МИФИ», Москва*

# НЕКОТОРЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ФУНКЦИОНИРОВАНИЯ ИНТЕЛЛЕКТУАЛЬНЫХ ОБУЧАЮЩИХ СИСТЕМ

Рассматриваются некоторые аспекты информационной безопасности функционирования интеллектуальных обучающих систем, разработанных на основе задачно-ориентированной методологии построения интегрированных экспертных систем и средств инструментального комплекса АТ-ТЕХНОЛОГИЯ.

Обучающие интегрированные экспертные системы (ИЭС) и веб-ИЭС, разработанные в лаборатории «Интеллектуальные системы и технологии» кафедры «Кибернетика» НИЯУ МИФИ, стали неотъемлемой частью учебного процесса и активно применяются с 2008 г. для автоматизированной поддержки базовых дисциплин по направлению подготовки «Программная инженерия», в том числе: «Введение в интеллектуальные системы и технологии», «Интеллектуальные диалоговые системы», «Динамические интеллектуальные системы», «Современные архитектуры интеллектуальных систем», «Проектирование систем, основанных на знаниях».

Созданные на основе авторской (Г.В. Рыбина) задачно-ориентированной методологии построения ИЭС и инструментального комплекса АТ-ТЕХНОЛОГИЯ обучающие ИЭС и веб-ИЭС являются полнофункциональными интеллектуальными обучающими системами (ИОС), обеспечивающими реализацию всех базовых моделей ИОС (модель обучаемого, модель обучения, модель проблемной области, онтологии курсов/дисциплин и др.), а также решение комплекса задач интеллектуального обучения (индивидуальное планирование методики изучения учебного курса/дисциплины; интеллектуальный анализ решения учебных задач; интеллектуальная поддержка принятия решений).

На все оригинальные авторские методики, реализованные в обучающих ИЭС и веб-ИЭС, получены свидетельства о государственной регистрации программ для ЭВМ, а для проведения практических занятий написаны новые учебные пособия [1, 2]. Мониторинг процессов функционирования обучающих ИЭС и веб-ИЭС проводится исходя из требований к надежности и информационной безопасности систем.

Приведем примеры процессов, в рамках которых возможны возникновения угроз безопасности. Режим RunTime: организация веб-тестирования (очное и дистанционное); выявление навыков/умений обучаемых решать различные задачи, в том числе неформализованные и др. Режим DesignTime: формирование заданий к элементам курсов/дисциплин; формирование и загрузка материалов для обучающих воздействий; анализ результатов мониторинга (в рамках анализа данных и т.п.).

Контроль доступа необходимо осуществлять для следующих информационных ресурсов, использующихся в процессах функционирования обучающих ИЭС: учетные и личные данные преподавателей и обучаемых, включая психологический портрет; варианты заданий для компонентов выявления уровня умений обучаемых; все элементы прикладных онтологий различных курсов/дисциплин, включая задания и вопросы к отдельным элементам курсов/дисциплин; сгенерированные варианты тестов, предназначенные для выявления уровня знаний обучаемых; описание заданий, ограничений и информационных ресурсы (изображения, файлы и др.), разработанных для обучающих воздействий; результаты выявления уровня знаний и умений обучаемых (ответы на вопросы, «проблемные зоны», ошибки и др.).

В рамках описанных процессов рассматриваются следующие варианты возможных угроз: DDoS-атаки для перегрузки ПО; MITM-атаки для похищения и/или подмены данных; попытки подобрать пароли или использовать украденные учетные данные (Brute Force и Credential Stuffing); злоупотребление правами доступа; загрузка вредоносных файлов;

Для обеспечения информационной безопасности в обучающих ИЭС применяются следующие подходы: использование защищенных сетевых протоколов с шифрованием; установка брандмауэров и сетевых профилей безопасности для фильтрации типов и протоколов подключений; ограничение доступа из внешних сетей в рамках проведения контрольных мероприятий (использование VPN, фильтрация IP-адресов и др.); анализ журналов и логов получения доступа к вариантам заданий и процессам выявления уровня знаний/умений обучаемых.

*Список литературы*

1. Рыбина Г.В. Интеллектуальные обучающие системы на основе интегрированных экспертных систем: учебное пособие. М.: Директ-Медиа, 2023. 123 с.

2. Рыбина Г.В., Григорьев А.А. Практические занятия по методам и технологиям построения динамических интеллектуальных систем: учебное пособие. М.: НИЯУ МИФИ, 2024. 140 с.