К ВОПРОСУ ИСПОЛЬЗОВАНИЯ ПЛАТФОРМЫ CTFd ДЛЯ ПОДГОТОВКИ СПЕЦИАЛИСТОВ ПО КИБЕРБЕЗОПАСНОСТИ

Т.Н. Гуцко, А.Ю. Суботковская

Capture the Flag или CTF в подготовке специалистов по кибербезопасности – это соревнования в форме командной игры. Участники решают прикладные задачи, чтобы получить уникальную комбинацию символов (флаг). Далее участники отправляют флаг в специальную форму и получают подтверждение, что задача решена верно или стоит попытаться дать ответ еще раз. CTF-турниры традиционно проводятся в двух форматах: в формате Task-Based (или Jeopardy), когда игрокам предоставляется набор заданий, к которым требуется найти и отправить ответ. Или в формате Classic (или Attack-Defense), когда участники получают идентичные серверы с набором уязвимых сервисов, на которых необходимо найти приватную информацию – флаги.

Надо отметить, что если в условиях проведения CTF-соревнований говорить о нарушениях не приходится, то при попытке использовать CTF в учебном процессе отмечаются постоянные нарушения академических требований – использования чужих флагов, передача решений другим участникам, несанкционированная коллективная работа и прочее, что не позволяет получить адекватную картину усвоения студентами материала и формирования у них необходимых компетенций.

Решением данной проблемы стал пакет на языке Python, используемый для анализа базы данных платформы CTFd и методика его применения с целью анализа работы академической группы и поиска инцидентов нарушения академических требований учебного процесса. База данных платформы представлена в виде файлов в json-формате. Основные данные, используемые для анализа, связаны с активностью участников и включают идентификаторы участника и его команды, задачи и время отправки флага, ip-адрес участника, сам флаг. Важные характеристики анализа: выбор периода рабочего времени, приоритет задач, динамика работы и пр.

Использование пакета предоставило преподавателю инструмент для анализа хода и динамики учебного процесса, а также подтвердило существенное повышение уровня сознательности и ответственности обучаемых. Платформа CTFd развернута с 2021 г. на платформе облачного кластера Гродненского государственного университета им. Янки Купалы (http://ctf.mf.grsu.by).