ФОРМИРОВАНИЕ ОБРАЗОВАТЕЛЬНОГО КОНТЕНТА ПО ОТКРЫТЫМ ИСТОЧНИКАМ МЕТОДАМИ АНАЛИТИЧЕСКОЙ РАЗВЕДКИ

И.М. Салей, Г.В. Щиглинский

События последнего времени, связанные с приостановкой работы на белорусском рынке некоторых ведущих ИТ-компаний, остро ставят вопрос о поддержке организаций, пользовавшихся их продуктами и сервисами. Так уход с белорусского рынка компании Cisco, привел к внезапной блокировке ресурсов программы Сетевых академий Cisco, участником которой белорусские университеты были почти 20 лет. Поэтому эксперты все активнее выступают за снятие ограничений на использование интеллектуальной собственности в современных условиях, предупреждая одновременно о рисках для участников рынка легального программного обеспечения.

В докладе представлен подход, использующий методы аналитической разведки, позволяющий на основе открытого контента интернет-ресурсов образовательного характера (наборы связанных веб-страниц, интерактивные учебные веб-ресурсы) формировать контент в традиционном академическом «бумажном» представлении (книги, методические пособия).

Использованный метод проведения аналитической разведки и извлечения информации предполагает выполнение ряда этапов. 1. Исследование технической составляющей сайта: анализ доменного имени, изучение структуры сайта, изучение использованных способов адресации и структуры ссылок на страницы сайта. 2. Исследование контента сайта: используемого шаблона страницы; структуры и стилей текстовой информации; принципов формирования графического контента сайта; идентификации тегов текстовой и графической части, элементов шаблона страницы; наличия дополнительных разделов. 3. Использование пакета скриптов на языке Python с доступом к библиотекам requests, bs4, selenium для извлечения контента. 4. Использование скриптов на языке Visual Basic for Application пакета MS Office для формирования «бумажных» аналогов полученного образовательного контента.

Работа проводилась в академических целях. Авторы разделяют авторитетное мнение, что «чтобы обеспечить защиту от атак, специалисты по кибербезопасности должны обладать теми же навыками, что и хакеры» [1].

Литература

1. Cybersecurity Essentials / Cisco Networking Academy [Electronic resource]. – Access mode: https://contenthub.netacad.com/ legacy/CyberEss/1.0/ru/course/module1/ 1.5.2.2/1.5.2.2.html. – Date of access: 03.05.2022.