3. Закон Украины «Об авторском праве и смежном праве» (в редакции Закона № 2627-III от 11.07.2001 // Ведомости Верховного Совета, 2001. № 43. Ст. 214.

ФОРМИРОВАНИЕ ЭЛЕКТРОННОЙ БИБЛИОТЕКИ ПО ВОПРОСАМ РАЗВИТИЯ «ЭЛЕКТРОННОГО ГОСУДАРСТВА»: ЗАДАЧИ ИНТЕГРАЦИИ ИНФОРМАЦИОННЫХ РЕСУРСОВ

И.А. Мбого, А.В. Чугунов
Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
Санкт-Петербург

Формирование научных коллекций в значительной степени проходит спонтанно и зависит в первую очередь от необходимости обеспечить информационную поддержку исследовательской или образовательной деятельности. К сожалению, в большинстве создаваемых электронных коллекциях не только отсутствует механизм обмена метаданными, но и сами метаданные в каком-либо из международных форматов.

В докладе представлен опыт реализации полнотекстовой электронной коллекции «Электронное государство», интегрированной с информационно-методическим порталом Центра технологий электронного правительства НИУ ИТМО (http://egov-center.ru).

Для создания электронной библиотеки «Электронное государство» в качестве базовой была выбрана система управления контентом Drupal, библиографический модуль biblio и модуль OAI-PMH. Выбор был основан на том, что эта система является не узкоспециализированной библиотечной системой, такой как DSpace или Eprints, а имеет значительные функциональные возможности по созданию различных, в том числе и мультимедийных коллекций, расширяя свой функционал за счет дополнительных модулей. Такой подход позволяет строить полнофункциональные коллекции с встроенной возможностью поддержки метаописаний.

Существует довольно много форматов описания метаданных, таких как MARC21, RUSMARC, USMARC. Приведенные форматы являются широко распространенными, но весьма сложными. В целях упрощения создания метаописания, унификации, согласования с протоколами обмена метаданными основным форматом обмена метаданными было решено использовать формат DublinCore.

Любая коллекция может быть построена как на базе многоуровневых классификаторов, так и без них. Формирование записей осуществляется на основании заполнения полей форм с привязкой к разделу классификатора. В качестве описываемых ресурсов могут выступать различные печатные издания (книги, статьи, авторефераты), электронные издания, артефакты реального мира. Поля формы поддерживают все типы данных Dublin Core и включают дополнительные возможности для расширенного описания. В качестве дополнительной опции реализована возможность формирования библиографического описания в соответствии с ГОСТ 7.1 – 2003 в полуавтоматическом режиме. Описание формируется на основании анализа заполненных полей и вставляется в дополнительное поле. Такой подход позволяет вручную скорректировать библиографическое описание в случае обнаружения неточности. В публикацию может быть включен полный текст в формате HTML или в виде прикрепленного файла. Любая запись может сопровождаться набором ключевых слов.

Библиографический модуль позволяет управлять отображением списка записей по нескольким параметрам – заголовок, автор, год, тип, ключевые слова. В дополнение к различным способам сортировок реализован набор фильтров, позволяющий организовать поиск по параметрам – по автору, по типу записи, по разделам классификатора, по годам, по ключевым словам.

Интеграционная система использует протокол OAI-PMH , который определяет механизм сбора записей, содержащих метаданные из различных хранилищ. Протокол предоставляет возможность хранилищам сделать метаданные доступными для сервисов, основанных на открытых стандартах HTTP и XML. Модуль OAI-PMH динамически формирует XML на все типы запросов протокола в нотации Dublin Core.

Использование данной методологии и технологий позволяет регистрировать ресурсы электронной коллекции в глобальных системах-сборщиках данных OAI (harvesters), например, таких как: scirus (http://www.scirus.com), myOAI (http://www.myoai.com), OAIster (http://oaister.umdl.umich.edu). Эти системы обеспечивают поиск научных публикаций, кумуляцию и взаимообмен данными между большей части университетов и исследовательских организаций всего мира.

Подсистема оперативного информирования участников профессионального научного сообщества будет поддерживать следующие функциональные возможности: ведение списков рассылки; индивидуальное информирование о новых поступлениях в электронную библиотеку и другие подсистемы; информирование о размещении электронной публикации в закрытой зоне; информирование о мероприятиях определенной направленности и т.п.

Проект предполагает работу с тремя группами пользователей:

- авторы научных публикаций - инициаторы (модераторы) тем научных дискуссий, члены редколлегий, рецензенты и редакционные работники (зарегистрированные пользователи со специфическим набором прав доступа к материалам и разделам системы);
- научные работники и преподаватели, заявившие о заинтересованности участия в сетевых обсуждениях и публикациях своих материалов, потенциальные авторы получающие доступ к неопубликованным рабочим материалам системы (зарегистрированные пользователи со стандартными правами);
- незарегистрированные пользователи, имеющие возможность ознакомиться с материалами, находящимися в открытом доступе.

Работа выполняется поддержке Российского фонда фундаментальных исследований (грант 11-07-00555-а).

ИСПОЛЬЗОВАНИЕ ОБМАННЫХ СИСТЕМ ДЛЯ ЗАЩИТЫ ЛОКАЛЬНОЙ СЕТИ ОРГАНИЗАЦИИ ОТ ВНЕШНИХ УГРОЗ

О.Ю. Пескова, В.М. Шериева
Таганрогский технологический институт Южного федерального университета (ТТИ ЮФУ)
Таганрог

ВВЕДЕНИЕ

Давно прошли времена, когда подключение организации к сети Интернет служило в основном для развлечения сотрудников, а в лучшем случае – для обмена электронной почтой. Сейчас многие предприятия используют глобальную сеть как часть своей технологической цепочки: Интернет используется не только для сбора информации, но и для работы с централизованными базами данных (например, для заказов у поставщиков), для работы с клиентами (например, через веб-сервера), для объединения филиалов и удаленных подразделений в единую сеть, и так далее. Поэтому сейчас остро стоят вопросы максимально эффективной и гибкой защиты ресурсов локальной сети организации при ее подключении к глобальной сети.

Наиболее эффективной считается стратегия (и она же является самой распространенной), которая состоит в том, чтобы обнаруживать любые недочеты в системе защиты и тут же их устранять. Но проблема этого подхода в том, что он пассивный: противник же всегда впереди и активно атакует. Практически всегда у хакера есть возможность адекватно отреагировать на защитные меры, и поэтому потенциально атакуемая сторона, чтобы минимизировать риск вторжения, просто обязана играть на опережение. [1]

Один из методов, позволяющий осуществить эту идею, называется HoneyPot (от англ. — «горшочек с медом»). HoneyPot представляет собой специальным образом доработанную систему, которая подключается к Интернет в качестве приманки, и злоумышленник будет атаковать приманку вместо того, чтобы атаковать реальную сеть. В процессе взлома системы-приманки установленные на ней средства слежения и регистрации должны зафиксировать все подробности этого процесса. Подобные системы-ловушки используются и в исследовательских целях как средство сбора информации о методах и средствах проведения атак (собранная информация, в частности, позволяет обнаруживать новые и уникальные уязвимости и эксплоиты), и для защиты организаций от взлома («промышленные» ловушки) [2]. Назначение промышленных ловушек - предотвращение атаки, обнаружение атаки и информационная поддержка в организации адекватных действий по блокированию атаки. Такие ловушки могут предотвращать нападения за счет замедления или эффекта увязания (tarring) автоматизированных атак. Ловушки могут более эффективно обнаруживать атаки, поскольку порождают меньшее количество тревог, как истинных, так и ложных. [3]