УДК 021:004.056
DOI 10.20913/2618-7515-2019-1-47-50

ПРОБЛЕМЫ И РЕШЕНИЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЭЛЕКТРОННЫХ БИБЛИОТЕК

PROBLEMS AND SOLUTIONS FOR ENSURING INFORMATION SECURITY OF ELECTRONIC LIBRARIES

© ***Норматов Шербек Бахтиерович***
докторант, Ташкентский университет информационных технологий имени Мухаммада аль-Хорезми (ТУИТ), Ташкент, Узбекистан, shb.normatov@gmail.com

Normatov Sherbek Baxtiyorovich
Doctoral candidate, Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Tashkent, Uzbekistan, shb.normatov@gmail.com

Развитие информационных технологий привело к активизации обмена информацией на расстоянии, резкому увеличению скорости поиска данных, хранения и обработки большого объема информации. В то же время именно эти возможности породили такие проблемы, как несанкционированный доступ к информационным ресурсам, угроза безопасности библиотечных ресурсов, необходимость обеспечения защиты личной информации пользователей. Увеличение объема и ценности информационных научно-технических и образовательных ресурсов приводит к повышению угроз несанкционированного доступа к ним. И это требует создания надежных средств защиты информационных источников.

Ключевые слова: *электронная библиотека, информационная безопасность, оценка информационной безопасности, нечеткая модель соответствий*

Information technologies development has led to intensification of distant information exchange, sharp increase in the speed of data retrieval, storage and processing of large amounts of information. At the same time, just these opportunities gave rise to such problems as unauthorized access to information resources, threat to the library resources security, need to ensure the users' personal information protection. Extension in the volume and value of information scientific-technical and educational resources leads to an increase in the threats of unauthorized access to them. This requires the creation of reliable means of protecting information sources.

Keywords: *electronic library, information security, information security assessment, fuzzy correspondence model*

Как известно, существуют информационные ресурсы открытого доступа и ограниченного использования – последние требуют создания определенных условий и средств их защиты. Такие ресурсы нужно защищать от несанкционированного доступа, то есть необходимо обеспечить их конфиденциальность. Даже если информация предназначена для открытого использования, все равно требуется обеспечение ее целостности и доступности. Кроме того, некоторые ресурсы могут быть предназначены для ограниченного использования, для отдельных категорий пользователей. Нарушение информационной безопасности (ИБ) может привести к нарушению целостности сохраняемых данных, а это, в свою очередь, может привести к понижению доверия к владельцам, учредителям, сотрудникам учреждений, владеющих источниками, а также к экономическим потерям.

Ценная научно-техническая и образовательная информация (НТОИ) в наибольшей степени влияет на развитие не только науки, образования, но и экономики и бизнеса, а также общества в целом [1]. Поэтому проблемы защиты информации являются наиболее актуальными. Под НТОИ понимается лицензионная информация электронных библиотек (ЭБ), информационно-ресурсных центров, данные о патентах и изобретениях в информационных сетях, научная и образовательная литература.

Эффективное обеспечение безопасности информации во многом зависит от выбора средств защиты и способов, соответствующих ценности информационных ресурсов. В настоящее время имеется множество способов и средств защиты информации, но проблема определения ее ценности с точки зрения ИБ остается мало изученной. Развитие исследований по определению

ценности НТОИ, а также методов их защиты от несанкционированного доступа является важной задачей.

В науке имеется опыт по решению слабоформализуемых проблем – это системный подход к их решению и системный анализ объектов исследования. В системном анализе акцентируется внимание на трудностях формулировки задач, на способах преодоления этих трудностей. Исходя из этого были поставлены следующие задачи: а) выявление проблемы обеспечения безопасности НТОИ и оценка ее актуальности; б) определение целей электронных библиотек, формирование общей цели и задач системы защиты НТОИ; в) идентификация и оценивание НТОИ с точки зрения ИБ.

Приведенные выше задачи требуют создания в ЭБ системы обеспечения безопасности информации. В данную систему могут быть положены общие требования, обеспечивающие снабжение и постоянную сохранность следующих свойств информации ЭБ:
– предоставление законным пользователям свободного пользования ресурсами библиотек;
– целостность и доступность информационных ресурсов библиотек, воспроизводимых в информационных системах, хранящихся, а также отправляемых через каналы связи;
– конфиденциальность информации;
– неприкосновенность личных данных.

Актуальность проблемы обеспечения безопасности НТОИ выражается следующими причинами:
– резкое возрастание объема сохраняемой информации и численности пользователей ЭБ;
– возрастание важных общественных, экономико-стратегических активных свойств информации;
– относительно высокая цена средств, надежно обеспечивающих безопасность информации;
– несформированность моделей, способов и принципов обеспечения безопасности НТОИ;
– незначительные знания по ИБ у руководителей и сотрудников библиотек;
– нарушение систем безопасности при возможности использования последних научно-технических достижений и т. д.

Большинство библиотек часто не готовы к управлению компьютерными сетями и новыми технологиями, именно они должны быть хорошо осведомлены об ИБ. На сегодняшний день библиотеки, при использовании своей локальной системы, должны предусмотреть меры по убеждению клиентов в неприкосновенности их частной жизни и личной ИБ. К безопасности информации, учитывая большое количество пользователей, также выдвигается ряд требований, каждая группа пользователей имеет разные меры безопасности [2].

Задача формализации процесса обеспечения ИБ библиотек сводится к последовательной формализации описания угроз ИБ, ресурсов ЭБ, оценке уровня обеспечения ИБ, определению вариантов мероприятий по обеспечению ИБ и выбору оптимального варианта обеспечения ИБ.

Пусть $R = \left\{ R_{ij}^{k} \right\}$ – множество ресурсов библиотек (где k – класс ресурса, i – тип ресурса, j – имя ресурса);
$U = \left\{ U_{ij}^{k} \right\}$ – множество источников угрозы (где k – класс угрозы, i – тип угрозы, j – имя угрозы);
$W = \left\{ W_{ij}^{k} \right\}$ – множество мероприятий по обеспечению ИБ (где k – класс мероприятий, i – тип мероприятий, j – имя мероприятия).
Для определения мероприятий по обеспечению ИБ зададим нечеткое соответствие множеств U и $W : \Gamma = \left\{ U, W, F \right\}$, где F – функция принадлежности $U \times W$. Нечеткое соответствие $\tilde{\Gamma}$ зададим в виде ориентированного графа с множеством вершин $U \cup W$, каждая дуга которого обозначает функцию принадлежности $\mu_F \left(u_i ; w_j \right)$ (рис. 1). В матричном виде нечеткое соответствие $\Gamma = \left\{ U, W, F \right\}$ зададим с помощью матрицы инцидентности R_{Γ} [3].

Для определения вариантов мероприятий по обеспечению ИБ сформулируем задачу оптимизации по следующим критериям: известны стоимость ресурсов ЭБ, угроз, методов и средств защиты ресурсов от угроз: $c\left(r_{\sigma} \right)$, $c\left(u_i \right)$, $c\left(w_j \right)$.

Необходимо определить приемлемые риски при заданных значениях, минимальные затраты на обеспечение ИБ с учетом проведенной селекции.

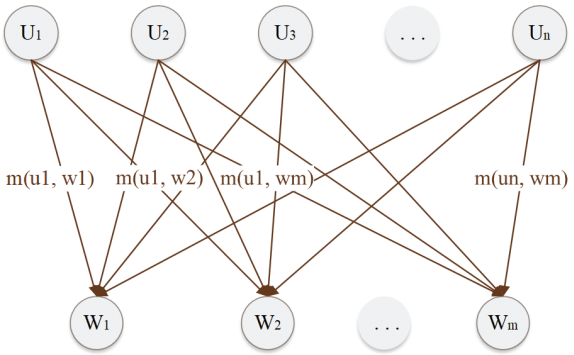

Рис. 1. Графическое задание нечеткого соответствия: $\Gamma = \left\{ U, W, F \right\}$

При этом введем ограничения: стоимость ресурса больше либо равна стоимости угрозы, направленной на него, в противном случае средства, затраченные на реализацию угрозы, экономически неоправданны. По той же причине стоимость ресурса больше либо равна стоимости мероприятий по его защите.

Исходя из поставленной задачи возникают вопросы оценки важности библиотечных ресурсов и угрозы их безопасности, а также вопросы соответствия мер безопасности угрозам.

Оценка важности информационных ресурсов представляется сложной задачей ввиду многокритериальности и неопределенности исходной информации, поэтому процедуру оценки важности информационных ресурсов будем строить с использованием концепции нечетких множеств [4].

Для оценки важности ресурсов зададим следующее: лингвистическая переменная $\Omega_R =$ «Важность ресурса с точки зрения ИБ организации», которая принимает нечеткие значения $D = \{D_1,\ D_2,\ D_3,\ D_4\}$, где $D_1 =$ «Незначимый»; $D_2 =$ «Значимый»; $D_3 =$ «Важный»; $D_4 =$ «Очень важный».

Для определения носителя множества Ω_R, содержащего терм-значения D, проведем балльный метод экспертной оценки. В качестве факторов, влияющих на оценку ресурса, используются следующие:

A_1 – стоимость ресурса (0 – низкая; 1 – средняя; 2 – высокая; 3 – очень высокая; 4 – критическая);

A_2 – важность ресурса в процессе функционирования всей информационной системы организации (0 – никак не влияет на работу других ресурсов; 1 – сбой в работе ресурса скажется на работе других ресурсов через некоторое время; 2 – сбой в работе ресурса скажется на работе незначительной части других ресурсов; 3 – сбой в работе этого ресурса делает неработоспособной значительную часть других ресурсов; 4 – сбой в работе ресурса приведет в нерабочее состояние всю систему);

A_3 – стоимость восстановления ресурса в случае его разрушения в результате реализации угрозы или комбинации угроз (0 – низкая; 1 – средняя; 2 – высокая; 3 – очень высокая; 4 – критическая);

A_4 – время восстановления ресурса в случае его разрушения в результате реализации угрозы или комбинации угроз (0 – до 1 часа; 1 – от 1 до нескольких часов; 2 – несколько суток; 3 – больше недели; 4 – около месяца);

A_5 – возможность восстановления ресурса в случае его утраты, частичного или полного разрушения (0 – легко; 1 – потребуются некоторые временные или/и материальные затраты; 2 – сложно (потребуются значительные временные и/или материальные затраты); 3 – очень сложно (потребуется недопустимо длительное время и/или недопустимые расходы на восстановление); 4 – невозможно);

A_6 – нарушение конфиденциальности (0 – малозначимо, нанесение морального ущерба в редких случаях; 1 – значимо, нанесение морального ущерба в определенных ситуациях; 2 – важно, незначительные материальные и/или моральные потери; 3 – очень важно, значительные материальные и/или моральные потери; 4 – критично, недопустимые материальные и/или моральные потери, крах работы);

A_7 – нарушение целостности (0 – незначимо, не влечет никаких последствий; 1 – значимо, последствия проявятся через некоторое время, но не приведут к сбою в работе; 2 – важно, последствия приведут к неправильной работе, обратимы; 3 – очень важно, последствия приведут к неправильной работе, необратимы; 4 – критично, неправильная работа всего ресурса, последствия модификации необратимы);

A_8 – нарушение доступности (0 – незначимо; 1 – значимо, работать можно, но использование экономит ресурсы; 2 – важно, работать можно, но использование потребуется; 3 – очень важно, работать можно короткое время; 4 – критично, работа останавливается). Из таблицы 1 следует, что носителем множества является отрезок [0 – 32].

Таблица 1

Матрица оценок носителя множества $\grave{U}_U$

Показатель	Терм-значение			
	D_1	D_2	D_3	D_4
A_1	0	1	1–2	3–4
A_2	0	0–2	1–3	2–4
A_3	0	0–1	1–3	2–4

Окончание таблицы 1

Показатель	Терм-значение			
	D_1	D_2	D_3	D_4
A_4	0–1	1–2	1–2	2–4
A_5	0–1	0–2	2–3	2–4
A_6	0–1	0–2	1–3	3–4
A_7	0–1	1–2	2–3	3–4
A_8	0–1	1–2	2–3	3–4
	0–5	**4–14**	**11–22**	**20–32**

График функции (рис. 2) отражает принадлежности терм-значений D_1, D_2, D_3, D_4 определенным интервалам.

Вышеуказанным методом можно оценить опасности угроз информационным ресурсам и определить меры их защиты.

Итак, возрастание объемов электронных библиотечных ресурсов, числа их пользователей, переход информации в важный актив, а также повышение попыток несанкционированных доступов к информации в свою очередь обостряет проблему обеспечения их безопасности. Таким образом, результат анализа проблемы обеспечения ИБ НТОИ показывает значимость приведенных данных и требует защиты от несанкционированного доступа.

Эффективность защиты НТОИ во многом зависит от соответствия методов и средств защиты ценности ресурсов. В настоящее время существует множество способов и методов защиты информации, таких как программные, технические, криптографические и т. д. Но при этом методы оценки защиты НТОИ все еще остаются не до конца изученными. На самом деле оценка защиты информационных ресурсов предоставляет возможность обладателям информации обращать внимание на вопросы, связанные с защитой информации, выделять денежные средства или экономить расходы.

С помощью предлагаемой модели можно оценить важность информационных ресурсов электронных библиотек.

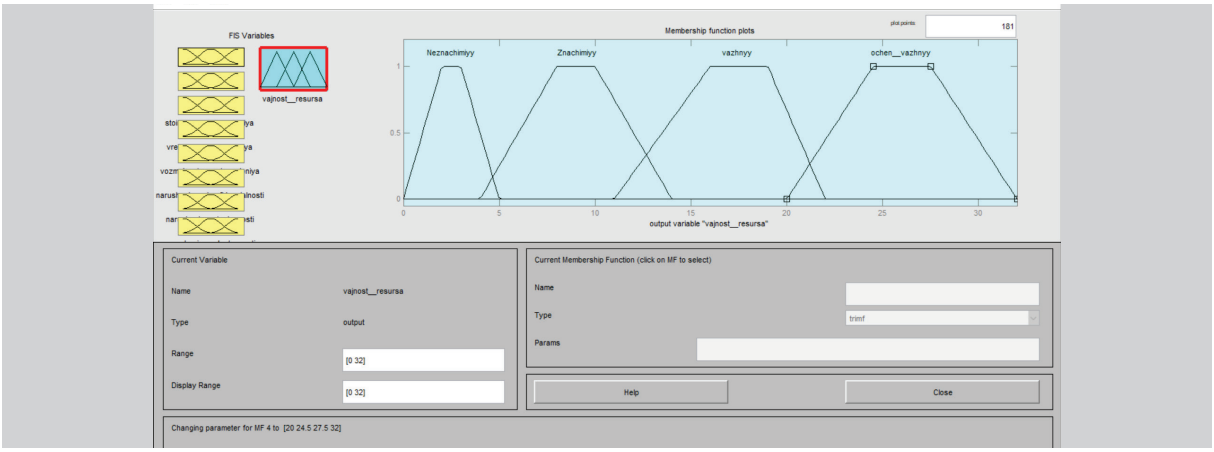

Рис. 2. Трапецеидальная форма оценки лингвистической переменной $\Omega_U =$ «Важность ресурса с точки зрения ИБ организации»

Список литературы

1. *Машкина И. В.* Управление защитой информации в сегменте корпоративной информационной системы на основе интеллектуальных технологий : дис. ... д-ра техн. наук. Уфа, 2009. 246 с.

2. *Ismail R., Zainab A. N.* Information systems security in special and public libraries: an assessment of status // Malaysian J. of Libr. & Inform. Science, 2011. Vol. 16, N. 2. P. 45–62.

3. *Кофман А.* Введение в теорию нечетких множеств в управление предприятиями : учеб. пособие. Минск : Выш. шк., 1992. 224 с.

4. *Рыжов А. П.* Элементы теории нечетких множеств и измерения нечеткости. Москва : Диалог-МГУ, 1998. 81 с.