https://doi.org/10.24108/2658-3143-2019-2-2-121-128

ОРИГИНАЛЬНЫЕ СТАТЬИ / ORIGINAL ARTICLES

Защита научно-образовательных ресурсов в информационно-библиотечных системах

Марат А. Рахматуллаев*, Шербек Б. Норматов

Ташкентский университет информационных технологий им. Мухаммада аль-Хоразмий
ул. А. Темура, 108, г. Ташкент, 100200, Узбекистан

Аннотация

Введение. В статье изложены результаты исследований по разработке методов и средств по обеспечению информационной безопасности научно-образовательных ресурсов в информационно-библиотечных системах и корпоративных информационных сетях. Приведен анализ состояния проблемы и существующих подходов обеспечения информационной безопасности электронных библиотек.

Материалы и методы. Обоснована необходимость защиты научных ресурсов от несанкционированного доступа и применения нечеткой логики для решения проблемы. Приведен анализ состояния проблемы и существующих подходов. В качестве модели и метода решения предлагается нечеткая модель соответствий второго рода, которая позволяет комплексно решить задачу определения угроз при возникшей ситуации, а также дать рекомендации по их устранению. Для формирования базы знаний привлекаются эксперты, которые определяют функции принадлежности в базе знаний «Ситуация — Угроза — Действия по устранению угроз».

Результаты исследования. Результаты исследований внедряются в составе программного комплекса информационно-библиотечной системы ARMAT++ корпоративной сети электронных библиотек 63 университетов Узбекистана для защиты научной и образовательной информации от несанкционированного доступа. Апробация методов, программ подсистемы и базы экспертных знаний проводится на базе информационно-ресурсных центров по проекту «Виртуальная электронная библиотека Ташкентского университета информационных технологий имени Мухаммада Ал-Хорезми и его филиалов».

Обсуждение и заключения. Применение аппарата нечеткой логики для формирования базы знаний вида «Ситуация — Угроза — Действия по устранению угроз» в информационно-библиотечных системах существенно повышает степень защиты ценных информационных ресурсов от несанкционированного доступа.

Ключевые слова: информационная безопасность, библиотечные системы, корпоративная сеть, научно-образовательные ресурсы, защита информации

Для цитирования: Рахматуллаев М.А., Норматов Ш.Б. Защита научно-образовательных ресурсов в информационно-библиотечных системах. *Наука и научная информация*. 2019;2(2):121-128. https://doi.org/10.24108/2658-3143-2019-2-2-121-128

Статья поступила: 24.03.2019
Статья принята в печать: 24.04.2019
Статья опубликована: 15.06.2019

Protection of Scientific and Educational Resources in Information and Library Systems

Marat A. Rakhmatullaev*, Sherbek B. Normatov

Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Temur str., 108, Tashkent, 100200, Uzbekistan

Abstract

Introduction. The authors of the article highlight the results of research on the development of methods and tools for ensuring the information security of scientific and educational resources in information library systems and corporate information networks. The analysis of the state of the problem and the existing approaches on this topic are given too.

Materials and Methods. The approach justifies the need to protect scientific resources from unauthorized access and the use of fuzzy logic to solve the problem. As a model and solution method, a fuzzy model correspondences is proposed, which makes it possible to comprehensively solve the problem of identifying threats in the event of a situation, as well as provide recommendations on how to eliminate them. For the formation of a knowledge base, experts are involved who determine the functions of belonging to knowlege base "Situation — Threats — Actions to eliminate the threats".

Results. The research results are being implemented as part of the ARMAT++ information library system of the corporate network of electronic libraries of 63 Uzbekistan universities for the protection of scientific and educational information from unauthorized access. Testing of the methods, programs of the subsystem and the expert knowledge base are carried out on the basis of information and resource centers under the project "Virtual electronic library of the Tashkent University of Information Technologies named after Muhammad Al-Khorezmi and its five branches".

Discussion and Conclusions. The use of the apparatus of fuzzy logic for the formation of a knowledge base of the "Situation — Threats — Actions to eliminate the threats" type in information library systems significantly increases the degree of protection of valuable information resources from unauthorized access.

Keywords: information security, library systems, corporate network, scientific and educational resources, digital library

For citation: Rakhmatullaev M.A., Normatov Sh.B. Protection of Scientific and Educational Resources in Information and Library Systems. *Scholarly Research and Information*. 2019;2(2):121-128. https://doi.org/10.24108/2658-3143-2019-2-2-121-128

Received: 24.03.2019
Revised: 24.04.2019
Published: 15.06.2019

1. Введение

Экспоненциальное увеличение объема информации привело к проблеме защиты финансовых, личных и государственных сведений. Информационная безопасность (ИБ) затронула не только финансовые сферы, но и политические. Поэтому задачи обеспечения ИБ требуют сегодня наибольшего внимания и потребляют наибольшее количество ресурсов в реализации проектов обработки, хранения и передачи информации. Эта проблема все больше касается и научной, научно-образовательной, научно-технической информации (далее НИ). Необходимость исследований по защите НИ и разработки новых методов, средств, проектов в этой сфере диктуется следующими факторами и тенденциями:

- резкое возрастание объема и количества пользователей научной информации;
- высокий уровень влияния результатов научных исследований на развитие технологий, военного производства, экономики и бизнеса, а также системы образования;
- противоречие между тенденциями предоставления все большего объема научной информации для различных слоев общества и желанием защитить ценные источники для собственных нужд;
- возрастание стоимости научной информации (электронных научных журналов, книг, баз данных и т. д.) и подписки на нее;

- развитие современных информационных технологий и средств телекоммуникаций, обеспечивающих доступ к электронным научным ресурсам как в локальных, так и в глобальных сетях;
- недостаточная осведомленность руководителей, специалистов организаций — собственников ресурсов о возможных угрозах, современных программно-технических средствах несанкционированного доступа и защиты от них;
- развитие информационных консорциумов (особенно библиотечных), объединенных для обмена ценной научной информацией.

Очевидно, что обладателями наиболее ценной научной и научно-образовательной информации являются библиотеки, а также компании, которые предоставляют услуги по доступу к научной информации. Библиотеки и библиотечные сети в наименьшей степени уделяют внимание информационной безопасности, т. к. их миссия противоречит самой сути ограничения доступа к их ресурсам. Анализ состояния развития исследований по защите научных ресурсов, ресурсов библиотек, информационных центров, издательств и агрегаторов показывает важность ИБ особенно в корпоративных информационных сетях и системах для обмена НИ. Корпоративные библиотечные сети включают десятки и даже сотни библиотек для активного информационного обмена, причем они (библиотеки) в разной степени оснащены средствами защиты информации.

Кроме того, НИ имеет специфические свойства по сравнению с другими видами информации:

- цена информационного ресурса изменчива. Причем один и тот же ресурс со временем может обесцениться, а может существенно повысить свой престиж и стоимость;
- разнообразие форм представления: от текста, таблиц, графической формы, до аудио, видео и др.;
- требование к целостности. Нарушение целостности комплекса научных данных может привести к неправильному пониманию научных результатов и их интерпретации;
- развитие конкуренции между производителями, обладателями информационных ресурсов;
- повышение стоимости научных информационных ресурсов как важного фактора продвижения экономики и бизнеса.

Целью исследований является повышение эффективности средств обеспечения информационной безопасности корпоративных библиотечных сетей и, соответственно, защита научной информации от несанкционированного доступа.

2. Материалы и методы

Информационно-библиотечные системы включают в себя такие общие активы, как базы данных, веб-сайты, устройства и программные приложения, управляемые администраторами систем и сетей [1]. Множество библиотек организовывают службу платных интерактивных услуг. Нередко в библиотечных системах, чтобы получить разрешения на использование библиотечных услуг, для регистрационной записи, читатели библиотек вводят свои личные данные, где указывают адрес, телефонные номера и другие личные сведения. Этот фактор способствует увеличению требований к безопасности [2]. Ни библиотека, ни читатели не заинтересованы в предоставлении «третьей» стороне личных данных. Актуально обеспечение безопасности систем электронного документооборота библиотек, электронных платежных систем и личных данных сотрудников и пользователей библиотеки [3, с. 21].

Увеличение объема конфиденциальной информации и изменение целей и задач людей, зависящие от постоянно развивающихся информационных и коммуникационных технологий, создают новые угрозы для научно-образовательных источников. Это, в свою очередь, усложняет проблему построения единой модели защиты от информационных угроз.

Вопросы защиты веб-ресурсов электронных библиотек подробно рассмотрены в трудах J. Kuzma и R. Ismail [4, 5]. Как отмечает Wilco, в некоторых случаях даже подписка на дорогостоящие базы данных может стать поводом для несанкционированного доступа к источникам [6]. S. Thompson и J. Kuzma указывают, что наиболее часто на практике атаки на НИ встречаются в виде XSS, DoS и SQL запросов [2, 4]. Нарушение информационной безопасности может привести к нарушению целостности сохраняемых данных, а это, в свою очередь, может привести к снижению уровня доверия к обладателю источника и соответствующим экономическим потерям.

Сами защищаемые объекты в библиотеках можно разделить на два вида: материальные и нематериальные (табл. 1).

Соответственно создаются как аппаратные, так и программные средства обеспечения ИБ. Методы и средства защиты информационных научно-образовательных ресурсов для таких известных информационных систем, как Auto-Graphics, Biblio Commons, Biblionix, EBSCO, SirsiDynix, OCLC, Ex Libris и Koha, представлены в [7]. R. Ismail рассматривает Library Information Security System Assessment Model (LISSAM) как один из вариантов решения проблемы [5].

Таблица 1. *Защищаемые объекты в информационно-библиотечных системах*
Table 1. *Protected objects in Information and Library systems*

Защищаемые объекты в информационно-библиотечных системах Protected objects in Information and Library systems	
Материальные / Tangible	Нематериальные / Intangible
• Специальное оборудование, компьютеры, серверы и сетевые устройства. • Носители данных (жесткие диски, оптические диски, флеш-память). • Средства физической защиты. • Аппаратные средства защиты.	• Электронный каталог. • Базы данных библиотечных ресурсов. • Персональные данные пользователей и сотрудников. • Программное обеспечение для обработки библиотечной информации (информационно-библиотечные системы). • Веб-сайт библиотеки (ресурсы сайта). • Информационные ресурсы, защищенные авторскими правами. • Информационные сервисы. • Информационные ресурсы о финансовом состоянии учреждения.

Эта модель выделяет меры безопасности и инструменты для технологической (безопасность программного обеспечения, оборудования, физической, сетевой безопасности, безопасности на рабочем месте и сервере) и организационной (политика информационной безопасности, мониторинг безопасности, методы и инструменты управления безопасностью, оценка состояния и прогнозирование) деятельности для информационно-библиотечных систем.

2.1. Формализация задачи обеспечения защиты информационных ресурсов (информационной безопасности в ИБС)

Задача формализации процесса обеспечения ИБ в ИБС сводится к последовательной формализации описания угроз ИБ, ресурсов, оценки уровня обеспечения ИБ, определения вариантов (видов) мероприятий по обеспечению ИБ и выбора из них оптимального (рационального) варианта.

Имеется множество $R = \{r_1, r_2, r_3 \ldots r_n\}$, которое включает все возможные условия состояния и оценки информационных ресурсов, где n — количество ситуаций.

r_i — могут быть: условия хранения ресурса; цена ресурса (установленная экспертами, стоимостью подписки или другими способами); условия доступа к информации (пароли, онлайн, в персональном компьютере, в локальной сети и др.); объем информации; вид документа и др.

Множество $T = \{T_{ij}^k\}\ (j = 1 \ldots m)$, которое включает все возможные угрозы для информационных ресурсов, где k — класс угроз, i — тип угроз, j — индентификатор угроз.

Имеется также множество $C = \{C_{ij}^k\}\ (j = 1 \ldots q)$, которое включает множество мероприятий по обеспечению ИБ при возникновении угроз, где k — класс мероприятия, i — тип мероприятия, j — индентификатор мероприятия.

$R_i \subset R$ является подсистемой R и включает только те условия состояния и оценки информационных ресурсов, которые свойственны конкретному объекту (библиотеке, фонду и др.). То есть фактически оно описывает конкретную ситуацию.

$T_{sj} \subset T$ — подмножество угроз, которое соответствует конкретной ситуации R_i; $C_{lj} \subset C$ — подмножество мероприятий по обеспечению ИБ при возникновении угроз T_{kj} для конкретной ситуации R_i.

Задача обеспечения информационной безопасности сводится к выявлению возможных угроз $T_{sj} \subset T$ для конкретного состояния (Ситуации) R_i, а также определению наиболее приемлемых мероприятий (Действий) $C_{lj} \subset C$ для их (Угроз) устранения.

На практике наиболее сложной задачей является определение соответствий между множествами R, T и C и, соответственно, формализованное

ее решение. Попытки решить задачу существующими детерминированными методами не дают положительных результатов.

Выбор методов нечеткой логики для оценки и защиты научной информации обосновывается следующими доводами:

1) невозможность сколь угодно точного измерения реальных величин по оценке информационного источника и других величин в изменяющихся условиях информационной среды. Например, сложно оценить цену научной информации на данный момент времени. Она варьируется в зависимости от спроса и уровня развития науки в данной области;
2) невозможность полного и четкого описания многих объектов и ситуаций. Для принятия решений по защите информации требуется определенный уровень формализации, наличие числовых оценок (пусть даже приближенных, но имеющих научное обоснование);
3) неточность функциональных действий, которые нередко не достигают поставленных системой целей. Многообразие научной информации, форм и методов ее формирования может затруднить создание адекватных средств как поиска, так и их оценки;
4) недостаточная размерность модели, не позволяющая отразить все значимые свойства объекта информационной среды. Не все параметры оценки единицы научной информации и показатели различных ситуаций, отражающие конкретную информационную среду, поддаются количественной оценке и строгой формализации. Требуются интуитивные оценки, учитывающие предыдущий опыт экспертов;
5) ненаблюдаемость ряда характеристик информационной среды, требующих интуитивных оценок.

Поэтому возникает необходимость в развитии методов, связанных с решением задач обеспечения информационной безопасности корпоративных информационно-библиотечных сетей, где исходная информация для принятия решений по защите ресурсов имеет расплывчатый характер. Применение методов теории нечетких множеств в решении этого класса задач оправдывается во многом и тем, что здесь в полной мере можно использовать ценный опыт, накопленный экспертами-специалистами в сфере информационно-библиотечной деятельности.

Функция принадлежности в теории нечетких множеств является ключевым понятием. Она ставит в соответствие каждому элементу $x_i \in X$ число из интервала [0;1], характеризующее степень принадлежности элемента x_i некоторому множеству A. Согласно Л. Заде функция принадлежности $\mu(x)$ является субъективной мерой того, насколько некоторый элемент $x_i \in X$ соответствует понятию, смысл которого формализуется нечетким множеством $A \subset X$ [8]. Эксперт, воспринимая информацию, не пользуется конкретными числами, а переводит их в свои понятия — значения лингвистической переменной. Каждое значение лингвистической переменной описывается функцией принадлежности $\mu(x)$, которая индивидуальна для каждого специалиста (эксперта).

Здесь под нечеткими моделями соответствий понимается формализованное описание объекта вида:

$$\tilde{\Gamma} = (R, T, \tilde{F}),$$

где R, T — четкие множества, характеризующие условия состояния и оценки информационных ресурсов и все возможные угрозы для информационных ресурсов соответственно.

$\tilde{F}$ — нечеткое множество в $R \times T$, характеризующее отношения между элементами r_i и t_j.

Нечеткое соответствие может быть задано теоретико-множественно, графически и в матричном виде.

Для решения задачи обеспечения информационной безопасности целесообразно в одной модели соответствий дать отношения между множествами R, T и C и привести к нечеткой модели соответствий 2-го рода (НМС 2-го рода), которая представляется в виде композиционного нечеткого соответствия [9]:

$$\tilde{G} = \tilde{\Gamma}1 \circ \tilde{\Gamma}2,$$

где $\tilde{\Gamma}1 = (R, T, \tilde{F}1)$,

$$\tilde{\Gamma}2 = (T, C, \tilde{F}2),$$

или $\tilde{G} = (R, T, C\ \tilde{F})$.

В композиционной НМС 2-го рода область отправления совпадает с областью отправления соответствия $\tilde{\Gamma}1$, а область прибытия — с областью прибытия соответствия $\tilde{\Gamma}2$, а график $\tilde{F}$ является композицией графиков $\tilde{F}1$ и $\tilde{F}2$.

В табличной форме представления НМС 2-го рода «Ситуация — Угроза — Действие» (табл. 2) можно наглядно показать соответствия между R, T и C, где μ — это функции принадлежности, которые устанавливает эксперт, соответственно для нечетких отношений между условиями R состояния и оценки информационных ресурсов и всеми возможными угрозами T для информационных ресурсов (в левой части таблицы), отношениями T к множе-

Таблица 2. *Нечеткая модель соответствий 2-го рода «Ситуация — Угроза — Действия по устранению угроз»*
Table 2. *A fuzzy second-type correspondences "Situation — Threat — Actions to eliminate the threats" model*

Признаки ситуации / Signs of the situations			Возможные угрозы / Possible threats		Действия по устранению угроз / Actions to eliminate the threats		
R_1	...	R_n			C_1	...	C_m
					$t_c^1 \dots t_c^l$	...	$t_c^1 \dots t_c^q$
$\mu < r_1, t_t^1 >$ $\mu < r_1, t_t^2 >$ ... $\mu < r_1, t_t^k >$	... ...	$\mu < r_n, t_t^1 >$ $\mu < r_n, t_t^2 >$ ... $\mu < r_n, t_t^k >$	T_1	t_t^1 t_t^2 ... t_t^k	$\mu < t_t^1, t_c^1 >$ $\mu < t_t^2, t_c^2 >$ ... $\mu < t_t^k, t_c^l >$	... ...	$\mu < t_t^1, t_c^1 >$ $\mu < t_t^2, t_c^2 >$ ... $\mu < t_t^k, t_c^q >$
...	...	...	...	...	...	...	...
$\mu < r_1, t_t^1 >$ $\mu < r_1, t_t^2 >$ ... $\mu < r_1, t_t^m >$	... ...	$\mu < r_n, t_t^1 >$ $\mu < r_n, t_t^2 >$ ... $\mu < r_n, t_t^m >$	T_m	t_t^1 t_t^2 ... t_t^m	$\mu < t_t^1, t_c^l >$ $\mu < t_t^2, t_c^l >$ ... $\mu < t_t^m, t_c^l >$	... ...	$\mu < t_t^1, t_c^q >$ $\mu < t_t^2, t_c^q >$ ... $\mu < t_t^m, t_c^q >$

ству возможных действий C. Такая форма представления удобна не только для наглядности соответствий, но и для выбора метода решения задачи.

3. Результаты исследования

Реализация НМС имеет конкретный прикладной аспект и предназначена для создания подсистемы «Информационная безопасность» для автоматизированной библиотечной системы ARMAT++, обеспечивающей корпоративное взаимодействие между шестьюдесятью академическими библиотеками Узбекистана.

В практической работе подсистемы «Информационная безопасность» предусмотрен ряд этапов:

1. Собирается информация о всех возможных ситуациях путем формулирования источников информации, угроз, методов и средств защиты и критериев оценки информационной безопасности. Выполняется оценка ресурсов, которые подлежат защите, угроз и защитных мер на основе экспертных оценок и статистических данных, критической оценки важности ресурсов, видов угроз и соответствия действия по устранению угроз или принятия мер по безопасности.
2. Формируется база знаний на основе оценок экспертов μ. Эксперты — в основном специалисты в сфере информационной безопасности, а также компетентные в оценке самих научных и образовательных информационных ресурсов. Эксперты устанавливают величины функций принадлежности отношений для $R \times T$ и $T \times X$. (т.е. по соответствиям типа «Ситуация — Угроза — Действия по устранению угроз»). Это является основой для формирования базы знаний. Для реализации модели НМС используется алгоритм обработки нечетких соответствий, описанный в работах М.А. Рахматуллаева [9, 10].
3. Для конкретной ситуации R_i определяются возможные угрозы $T_j \subset T$, а также определяются наиболее приемлемые мероприятия (Действия) $C_k \subset C$ для их (Угроз) устранения. В конечном итоге даются рекомендации для выполнения

совокупности действий, чтобы не допустить воздействия угроз или их устранить.

Программная реализация модели производится в рамках проекта разработки корпоративной информационно-библиотечной сети для 60 академических библиотек вузов Узбекистана в составе подсистемы «Информационная безопасность» библиотечной системы ARMAT++ [9].

4. Обсуждение и заключение

Увеличение объема, стоимости электронных библиотечных ресурсов и количества пользователей электронных библиотек, а также попыток несанкционированного доступа к информации привело к проблеме обеспечения безопасности библиотечных систем, особенно в корпоративных сетях.

Результаты исследования позволили сделать следующие выводы:

- анализ состояния существующих методов и средств обеспечения информационной безопасности показывает необходимость проведения исследований по применению методов нечеткой логики и нечеткого множества для решения задач защиты научных и образовательных ресурсов. Это объясняется тем, что не все параметры оценки единицы научной информации и показатели различных ситуаций поддаются количественной оценке, строго формализованы и требуют интуитивных оценок, учитывающих предыдущий опыт экспертов по выявлению реальных угроз и принятию соответствующих мер. Очевидно, что для принятия решений о защите информации необходим определенный уровень формализации, наличие числовых оценок. Хотя эти оценки могут быть приблизительными, они должны быть научно обоснованы и/или опираться на экспертные знания;
- приведение задачи информационной безопасности для информационно-библиотечных систем и корпоративных библиотечных сетей к формализованной нечеткой модели отношений с использованием аппарата нечеткой логики позволяет комплексно решать ее в отношениях «ситуация — угроза» и «угроза — действия по устранению угроз»;
- разработанная нечеткая модель отношений имеет важное практическое значение, ее программная реализация в составе подсистемы информационной безопасности корпоративной сети библиотек решает проблему обеспечения защиты источников научной информации в библиотеках.

СПИСОК ЛИТЕРАТУРЫ

1. Федякова Н.Н., Ивойлов Э.М., Табачников Р.А. Обеспечение информационной безопасности электронной библиотеки. URL: https://docplayer.ru/43934328-Obespechenie-informacionnoy-bezopasnosti-elektronnoy-biblioteki.html
2. Thompson S. Helping the hacker? Library information, security and social engineering. Information Technology and Libraries. 2006;25(4):222–225. https://doi.org/10.6017/ital.v25i4.3355
3. Rodionova Z.V., Bobrov L.K. Protection of the Information Resources of a Library Based on Analysis of Business Processes. Scientific and Technical Information Processing. 2016;43(1):20–27.
4. Kuzma J. European digital libraries: web security vulnerabilities. Library Hi Tech. 2010;28(3):402–413. https://doi.org/10.1108/07378831011076657
5. Ismail R., Zainab A.N. Information systems security in special and public libraries: an assessment of status. Malaysian Journal of Library & Information Science. 2011;16(2):45–62. URL: https://mjlis.um.edu.my/article/view/6697
6. Wilco E. Information Assets and their Value. 6th Twente Student Conference on IT, Enschede, 2nd February, 2007, University of Twente. URL: https://www.semanticscholar.org/paper/Information-Assets-and-their-Value-Engelsman/a9c3f38f978b124d077fa99fd169e5c2dfb28a65
7. Breeding M. The Current State of Privacy and Security of Automation and Discovery Products. Library Technology Reports. 2016;52(4):13–28. URL: https://journals.ala.org/index.php/ltr/article/view/5974/7608
8. Zadeh L.A. Fuzzy sets. *The Journal of Symbolic Logic*. 1973;38(4):656–657. https://doi.org/10.2307/2272014
9. Rakhmatullaev M. Increase of determinacy of information environment for intellectualization of information retrieval. Proceeding of International conference. WCIS 2014. Eighth World Conference on Intelligent Systems for Industrial Automation. 2014;329–334.
10. Рахматуллаев М.А. Композиционная модель соответствий для решения задач нечеткой технологической среды. *Автоматика и вычислительная техника*. 1993;6:33–40.

REFERENCES

1. Fedyakova N.N., Ivoylov E.M., Tabachnikov R.A. Ensuring the information security of the electronic library. Available at: https://docplayer.ru/43934328-Obespechenie-informacionnoy-bezopasnosti-elektronnoy-biblioteki.html (In Russ.).
2. Thompson S. Helping the hacker? Library information, security and social engineering. Information Technology and Libraries. 2006;25(4):222–225. https://doi.org/10.6017/ital.v25i4.3355
3. Rodionova Z.V., Bobrov L.K. Protection of the Information Resources of a Library Based on Analysis of Business Processes. Scientific and Technical Information Processing. 2016;43(1):20–27.
4. Kuzma J. European digital libraries: web security vulnerabilities. Library Hi Tech. 2010;28(3):402–413. https://doi.org/10.1108/07378831011076657
5. Ismail R., Zainab A.N. Information systems security in special and public libraries: an assessment of status. Malaysian Journal of Library & Information Science. 2011;16(2):45–62.
6. Wilco E. Information Assets and their Value. 6th Twente Student Conference on IT, Enschede, 2nd February, 2007, University of Twente. Available at: https://www.semanticscholar.org/paper/Information-Assets-and-their-Value-Engelsman/a9c3f38f978b124d077fa99fd169e5c2dfb28a65
7. Breeding M. The Current State of Privacy and Security of Automation and Discovery Products. Library Technology Reports. 2016;52(4):13–28. Available at: https://journals.ala.org/index.php/ltr/article/view/5974/7608
8. Zadeh L.A. Fuzzy sets. *The Journal of Symbolic Logic*. 1973;38(4):656–657. https://doi.org/10.2307/2272014
9. Rakhmatullaev M. Increase of determinacy of information environment for intellectualization of information retrieval. Proceeding of International conference. WCIS 2014. Eighth World Conference on Intelligent Systems for Industrial Automation. 2014;329–334.
10. Rakhmatullayev M. Compositional correspondence model for solving problems of a fuzzy technological environment. *Automatic Control and Computer Sciences*. 1993;6:33–40 (In Russ.).

ИНФОРМАЦИЯ ОБ АВТОРАХ / INFORMATION ABOUT THE AUTHORS

Марат Алимович Рахматуллаев, д-р техн. наук, профессор Ташкентского университета информационных технологий им. Мухаммада аль-Хоразмий;
marat56@mail.ru
ORCID: https://orcid.org/0000-0003-2587-1120

Шербек Бахтиерович Норматов, докторант Ташкентского университета информационных технологий им. Мухаммада аль-Хоразмий;
shb.normatov@gmail.com
ORCID: https://orcid.org/0000-0002-2563-0485

Marat A. Rakhmatullaev, Dr. Sci. (Engineering), professor, Tashkent University of Information Technologies named after Muhammad al-Khwarizmi;
marat56@mail.ru
ORCID: https://orcid.org/0000-0003-2587-1120

Sherbek B. Normatov, PhD student, Tashkent University of Information Technologies named after Muhammad al-Khwarizmi;
shb.normatov@gmail.com
ORCID: https://orcid.org/0000-0002-2563-0485