ISSN 2686-679X

ВЕСТНИК РГГУ

Серия
«Информатика.
Информационная безопасность.
Математика»

Научный журнал

RSUH/RGGU BULLETIN

"Information Science.
Information Security. Mathematics"
Series

Academic Journal

Основан в 2018 г.
Founded in 2018

4
2020

VESTNIK RGGU. Seriya «Informatica. Informacionnaya bezopasnost. Matematica»

RSUH/RGGU BULLETIN. "Information Science. Information Security. Mathematics" Series
Academic Journal

There are 4 issues of the printed version of the journal a year.

Founder and Publisher
Russian State University for the Humanities (RSUH)

RSUH/RGGU BULLETIN. "Information Science. Information Security. Mathematics" series is included: in the Russian Science Citation Index; in the List of leading scientific magazines journals and other editions for publishing PhD research findings peer-reviewed publications fall within the following research area:

20.00.00 Informatics

81.03.29 Information security, data protection,

27.00.00 Mathematics

Objectives and areas of research

RSUH/RGGU BULLETIN. "Information Science. Information Security. Mathematics" series publishes the results of research by scientists from RSUH and other universities and other Russian and foreign academic institutions. The areas covered by contributions include theoretical and applied computer science, up-to-date IT, means and technologies of information protection and information security as well as the issues of theoretical and applied mathematics including analytical and imitation models of different processes and objects. Special emphasis is put on articles and reviews covering research in indicated directions in the areas of social and humanitarian problems and also issues of personnel training for these directions.

RSUH/RGGU BULLETIN. "Information Science. Information Security. Mathematics" series is registered by Federal Service for Supervision of Communications Information Technology and Mass Media. 25.05.2018, reg. No. FS77-72977

Editorial staff office: 6, Miusskaya sq., Moscow, Russia, 125993, GSP-3

tel: +7 (916) 250-90-85

e-mail: adkozlov@mail.ru

ВЕСТНИК РГГУ. Серия «Информатика. Информационная безопасность. Математика»

Научный журнал
Выходит 4 номера печатной версии журнала в год.
Учредитель и издатель – Российский государственный гуманитарный университет (РГГУ)

ВЕСТНИК РГГУ. Серия «Информатика. Информационная безопасность. Математика» включен в систему Российского индекса научного цитирования (РИНЦ); в Перечень рецензируемых научных изданий, в которых должны быть опубликованы основные результаты диссертаций на соискание ученой степени кандидата наук, на соискание ученой степени доктора наук по следующим научным специальностям и соответствующим им отраслям науки:

20.00.00 Информатика

81.93.29 Информационная безопасность, защита информации

27.00.00 Математика

Цели и область

В журнале «Вестник РГГУ», серия «Информатика. Информационная безопасность. Математика» публикуются результаты научных исследований ученых и специалистов РГГУ, а также других университетов и научных учреждений России и зарубежных стран. Направления публикаций включают теоретическую и прикладную информатику, современные информационные технологии, методы, средства и технологии защиты информации и обеспечения информационной безопасности, а также проблемы теоретической и прикладной математики, включая разработку аналитических и имитационных моделей процессов и объектов различной природы. Особое внимание уделяется статьям и обзорам, посвященным исследованиям по указанным направлениям в области социальных и гуманитарных проблем, а также вопросам подготовки кадров по соответствующим специальностям для данных направлений.

ВЕСТНИК РГГУ. Серия «Информатика. Информационная безопасность. Математика» зарегистрирован Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций 25.05.2018 г., регистрационный номер ПИ № ФС77-72977.

Адрес редакции: 125993, ГСП-3, Россия, Москва, Миусская пл., 6

Тел: +7 (916) 250-90-85

электронный адрес: adkozlov@mail.ru

Учредитель и издатель
Российский государственный гуманитарный университет (РГГУ)

Ответственный за выпуск:

А.Д. Козлов, кандидат технических наук, доцент (РГГУ)

Contents

Содержание

УДК 004:130.2
DOI: 10.28995/2686-679X-2020-4-8-18

Принципы цифровизации сохранения культурного наследия

Наталья В. Лопатина

Московский государственный институт культуры,
Москва, Россия, dreitser@yandex.ru

Аннотация. В работе поставлена научная задача актуализации теоретических оснований цифровизации сохранения культурного наследия. Проведен анализ современных рисков, определяющих необходимость модернизации подходов к сохранению культурного наследия. Представлены уровни, подходы, инструменты сохранения культурного наследия в условиях цифровой трансформации культурного развития и культурных практик. Конкретизированы задачи и обозначены ключевые направления прикладной информатики в культуре, связанные с цифровизацией сохранения культурного наследия. Представлены 4 группы принципов цифровизации сохранения культурного наследия: технологические принципы, организационные принципы, специализированные принципы отраслевой цифровизации, принципы эффективности проектов цифровизации. Группа технологических принципов включает принцип соответствия стандартам, масштабируемость применяемых методов и решений, принцип диалектики универсальных и профессионально-ориентированных ИТ-решений. Группа организационных принципов включает принцип единства цифрового пространства культуры, принцип координации в цифровизации сохранения культурного наследия, принцип стратегического единства. Специализированные принципы отраслевой цифровизации выделены в силу особенностей экономического и цифрового развития сферы культуры. Принципы эффективности проектов цифровизации определяют целесообразность инвестиций в цифровизацию сохранения культурного наследия. Цифровизация культурного наследия – это совокупность новых ИТ-решений, нового дизайна информационного пространства культуры, новых отношений в профессиональной и социальной среде, новые экономические модели.

Ключевые слова: цифровизация, прикладная информатика культуры, сохранение культурного наследия, цифровая гуманитаристика

Для цитирования: Лопатина Н.В. Принципы цифровизации сохранения культурного наследия // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика» 2020. № 4. С. 8–18. DOI: 10.28995/2686-679X-2020-4-8-18

Principles of digitalization for the cultural heritage preservation

Natalia V. Lopatina
Moscow State Institute of Culture, Moscow, Russia, dreitser@yandex.ru

Abstract. The paper sets a scientific problem of updating the theoretical foundations for digitalization of the cultural heritage preservation. It carries out an analysis of modern risks that determine the need to modernize approaches to the preservation of cultural heritage and presents the levels, approaches, and tools for preserving cultural heritage in the context of digital transformation of cultural development and cultural practices. The tasks and key areas of applied informatics in culture related to the digitalization of cultural heritage preservation are specified. Principles of digitalization for the cultural heritage preservation are presented in four groups: technological principles, organizational principles, specialized principles of sectoral digitalization, principles of the digitalization projects effectiveness.

The group of technological principles includes the compliance with standards, scalability of the applied methods and solutions, and the dialectics principle of universal and professionally oriented IT solutions. The group of organizational principles includes the unity principle for the digital space of culture, the coordination principle for the digitalization of cultural heritage preservation, and the principle of strategic unity. Specialized principles of sectoral digitalization are highlighted due to the nature of economic and digital development in the cultural sphere. The effectiveness principles for the digitalization projects determine the feasibility of investing to digitalization for the cultural heritage preservation. Digitalization of cultural heritage is a combination of new IT solutions, new design of the cultural information space, new relationships in the professional and social environment, and new economic models.

Keywords: digitalization, applied informatics of culture, cultural heritage preservation, Digital Humanities

For citation: Lopatina, N.V. (2020), "Principles of digitalization for the cultural heritage preservation", *RSUH/RGGU Bulletin. "Information Science. Information Security. Mathematics" Series*, no. 4, pp. 8–18, DOI: 10.28995/2686-679X-2020-4-8-18

Введение

Сохранение культурного наследия как совокупности материальных и духовных ценностей, созданных предыдущими поколениями и транслирующих традиции, запас знаний, культурные коды, выступает одним из магистральных направлений управления культурой в современном мире [Ярилова 2008]. Специфика внешних факторов (природных, антропогенных, социально-информационных) позволяет говорить о своевременности подобных решений в силу рисков различной природы.

С одной стороны, это риски естественной утраты и естественного старения объектов культурного наследия, в том числе усиление этих рисков вследствие ухудшения экологической обстановки и цифровых трансформаций культурного пространства. С другой стороны, гуманитарные приоритеты развития современного общества формируют риски массового социального потребления объектов культурного наследия, в первую очередь тех моделей потребительского поведения, которые базируются на безнаказанности, варварстве, культурном нигилизме. С третьей стороны, существуют риски, обусловленные пониманием и упреждением вышеописанных рисков, что выражается в ограничении доступности объектов культурного наследия населению с целью их физической сохранности. С четвертой стороны, риски преувеличения возможностей цифрового инструментария и новых режимов социальных коммуникаций для выявления, изучения и сохранения и материального, и нематериального культурного наследия.

В этой связи не теряет актуальности вопрос о развитии арсенала методов сохранения культурного наследия – в русле киберфизической концепции информационно-технологического проектирования. Сегодня даже неспециалисту понятно, что новый виток развития культуры в условиях информатизации связан с интеграцией мейнстримных нововведений: моделирования и симуляторов, Интернета вещей, дополненной реальности, 3D-печати, имитационного моделирования и т. д. Следует отметить значительные изменения профессионального сознания как представителей институтов сохранения культурного наследия и институтов памяти, так и информационных специалистов, их открытость построению композитного мира, который еще совсем недавно представлялся невозможным. Вместе с тем это взаимодействие требует не только преодоления психологических, организационных, экономических и информационно-технологических барьеров. Необходима своего рода идеологическая платформа, направляющая и регулирующая приложения инструментов и положений теоретической информатики для решения практических задач в сфере культуры – с одной

стороны, информогенной отрасли – с другой, уникальной по своей структуре, организационному оформлению, механизмам экономики и потребления.

Процессы сохранения культурного наследия и их цифровизация

Анализ проектов цифрового развития культуры показывает, что проблемный характер настоящей ситуации заключается в слабой взаимосвязи теоретических изысканий и технического поиска, в интуитивности и отсутствии научной обоснованности многих проектов, что, в конечном итоге, порождает точечный характер, отсутствие стратегической ориентации, несовместимости различных проектов информатизации сохранения культурного наследия.

Сложившийся до информационной эпохи классический подход к сохранению культурного наследия включает 4 основных процесса – консервация, ревалоризация, реставрация, музеефикация, которые можно считать фундаментальными, ибо многочисленные технологические и социально-экономические изменения последних десятилетий подтвердили их временную универсальность и устойчивость. Вместе с тем цифровое развитие расширяет представления об уровнях, подходах, инструментах сохранения культурного наследия и ставит новые задачи перед разработчиками следующих информационно-технологических решений.

Во-первых, виртуализация непосредственных контактов с культурной средой переходит от создания «параллельной действительности», «информационного инобытия», моделирующей основные объекты культурного наследия, к формированию системы связей с реальностью, которые способны отражать многообразие профессиональных манипуляций с ними, исследовательских процессов, их освоение и популяризацию. При этом «новые компьютерные возможности лишь инициировали и актуализировали древнейшие способы информационного отражения реальности и информационных коммуникаций, доминировавшие в довербальную эпоху» [Сляднева 1999]. Именно эта реконструируемая и воссоздаваемая посредством новых технологий система связей формирует зону пересечения сред – реальной и информационной. Эту зону и рассматривают апологеты «четвертой промышленной революции» как явление новое не только по реализации, но и по идее, хотя человечество всегда обитало в двух измерениях – в физическом, «вещном» мире и в информационном пространстве, отражающем и моделирующем реальное бытие.

Во-вторых, история развития информационных технологий («информационная история») демонстрирует поступательное усиление в повседневных практиках «знания без субъекта знания», «третьего мира» (наряду с миром физических объектов и миром мышления), где обитают знания «без субъекта знания» [Поппер 2002]. Эти изменяющиеся практики создают и транслируют расширяющее понимание культурного наследия, интегрируют новые форматы сохранения культурного наследия, выходящие за рамки центризма материальных носителей культурных кодов (например, нематериальное культурное наследие, традиционные знания и культуры [Неретин 2018]); формируемое («будущее») цифровое культурное наследие [Лопатина, Неретин 2018]; сохранение культурного наследия вне традиционных документных форм (распределенные реестры, свернутое знание, формулы объектов интеллектуальной собственности).

В-третьих, единое информационное пространство культуры как теоретический концепт и стратегический ориентир ставит новые задачи сохранения культурного наследия, которые концентрируются не только на отражении дискретных, но и системных объектов (национальных, по времени, художественным и идеологическим течениям, отраслям культуры и т. д.). Основная задача – построение культурного континуума, отражение и сохранение не только отдельных объектов культурного наследия, но и контекста их появления и бытования, а также тех информационных по своей природе связей, которые позволяют говорить о культурном наследии как о системе.

В-четвертых, трансформации общества в ходе цифрового развития усиливают полиакторность развития. Высокий уровень диффузии новых информационно-коммуникативных форматов в профессиональные и массовые культурные практики усиливает возможности культурного и гуманитарного просвещения как особого фактора и формы сохранения культурного наследия, создает условия для инициативных цифровых проектов, для консолидации усилий и ресурсов стейкхолдеров сохранения культурного наследия [Неретин 2015].

Современный этап цифрового развития усиливает социальную активность массового субъекта сохранения культурного наследия. Стимулируются организация и самоорганизации коллабораций по поиску и выявлению объектов культурного наследия, интеграции данных о них в единые информационные системы, по продвижению в социальных сетях (например, проект «Руиннет» – «портал народного мониторинга призван дать возможность тем, кому небезразлична судьба памятников, храмов, усадеб и других объектов, имеющих культурную ценность, помочь сохранить эти

объекты и собрать как можно больше информации об их текущем состоянии»[1]). Вместе с тем участие массового актора усиливает риск дилетантизма, несанкционированных информационных манипуляций в цифровом культурном пространстве, что ставит принципиально новые задачи в русле прикладной информатики в культуре. С одной стороны, это экстраполяция в новые разработки уже ставших традиционными методологий информационной безопасности.

С другой стороны, история культуры, реконструкция культурных контекстов и организационных моделей сохранения культурного наследия определяют риски субъектной концентрации в процессах принятия решений, касающихся сохранения культурного наследия, в первую очередь в определении социальной и культурной значимости отдельных явлений, событий, персон. В этой связи встает принципиально новая задача для теории и практики прикладной информатики в культуре – достижение оптимального взаимодействия между инструментарием «субъектной» экспертизы (где профессиональное культурологическое и искусствоведческое знание эксперта микшируется с его эмоциями, интуицией, ощущением времени и ситуации, когнитивным стилем, идентификацией) и экспертизой на базе искусственного интеллекта, кумулирующего, организующего и систематизирующего коллективное знание. Построение таких систем в помощь современным специалистам в области сохранения культурного наследия, стейкхолдерам – задача первого уровня. Задача следующего уровня – их наполнение культурологическим и искусствоведческим знанием, художественной информацией, что требует выработки и формализации специфических, информационно-отраслевых, подходов к отбору, организации, представлению, аналитико-синтетической переработке.

В этой связи необходимо определить принципы цифровизации сохранения культурного наследия как условия единства стратегических ориентиров и создания единого антирискового пространства, что позволит разработать наиболее эффективные решения и интегрировать их в разнообразные системы культурного наследия. Именно основные принципы как теоретическая основа цифровизации сохранения культурного наследия определят ее методы. Данный вопрос получал рассмотрение в работах [Войтин, Тютюнник 2014], [Тютюнник, Войтин, Тявкин 2016], однако характер цифрового развития и его влияние на конфигурацию сферы культуры и управление цифровизацией отрасли требуют регулярной ревизии исходных положений (принципов).

[1] Руиннет [Электронный ресурс]. URL: https://ruin.net.ru (дата обращения 10 декабря 2020).

Принципы цифровизации сохранения культурного наследия

Основные принципы цифровизации сохранения культурного наследия целесообразно разделить на три группы: технологические принципы, организационные принципы, специализированные принципы отраслевой цифровизации, принципы эффективности проектов цифровизации.

К технологическим принципам относятся:

1. Принцип соответствия стандартам как условия технологической и кадровой преемственности и основы технологизации креативных цифровых решений. Особую роль принцип стандартизации играет в формировании единого цифрового пространства культуры и вхождения России в международные проекты цифровизации сохранения культурного наследия.
2. Принцип рациональности в определении приоритета «готовое решение» / «креативное (оригинальное, вновь созданное) решение». Для сокращения сроков внедрения и уровня сопутствующих рисков, что особенно важно для объектов культурного наследия, в случае равноценного выбора между созданием системы и использованием коммерческого или ранее созданного, проверенного и поддерживаемого решения, в большинстве случаев приоритетным является решение о приобретении и адаптации «готового» решения. Вместе с тем реализация масштабных проектов, новых по идее, по отраслевым задачам, определяет целесообразность движения вперед, поиска решений.
3. Масштабируемость применяемых методов и решений. Разрабатываемые решения должны предусматривать варьирование масштабов внедрения, интеграции либо исключения сервисов в зависимости от ресурсов проектов отраслевой цифровизации, от уровня готовности к цифровым преобразованиям, что актуально для сферы культуры.
4. Принцип диалектики универсальных и профессионально-ориентированных ИТ-решений.

Группа организационных принципов информатизации в большинстве научных публикаций представлена, во-первых, «хрестоматийными» принципами последовательности (этапности и непрерывности); направленности; эффективности; управляемости; открытости; ресурсной обеспеченности; преемственности. Эти принципы адекватны и для цифровизации сохранения культурного наследия. Вместе с тем стратегические ориентиры данной функции управления культурой требуют дополнения набора принципов. В первую очередь речь идет о принципе единства цифрового

пространства культуры, который ориентирует на обозначенные выше стратегические подходы построения единого цифрового пространства культуры и необходимые условия решения этой задачи (в том числе учет разнообразия пользователей). Во-вторых, принцип координации в цифровизации сохранения культурного наследия, что ориентирует на стандартизацию решений, регламенты системной интеграции, интеграции информационных ресурсов разных типов и видов.

Одним из основополагающих должен стать принцип стратегического единства, что предполагает выработку ИТ-стратегии не только на уровне отдельных организаций, но и на уровне всего рассматриваемого функционального направления управления культурой – сохранения культурного наследия. Этот принцип ориентирует на четкость целеполагания цифровых проектов сохранения культурного наследия и его понимания всеми участниками процесса, на обоснованность последовательности, длительности и стоимости шагов, на формирование эффективного взаимодействия ключевых направлений сохранения культурного наследия. Отсутствие единой стратегии, координирующей все направления функциональной отраслевой цифровизации, снижает эффективность точечных, разрозненных проектов и обуславливает типичную проблему несоответствия инвестированных ресурсов и эффекта, полученного от вложения в цифровые решения.

Группа специализированных принципов отраслевой цифровизации выделена в силу особенностей экономического и цифрового развития сферы культуры, управления ею. Фундаментальный характер культурного процесса определяет специфику социальной эффективности цифровизации сохранения культурного наследия, которая заключается в оппозиции экономической (финансовой) эффективности как критерия оценки цифровых проектов в бизнесе. В данном случае речь идет о социальном государстве как акторе управления культурой в целом и сохранения культурного наследия, в частности от уровня законодательных структур до массового потребителя культурных благ. Это определяет целесообразность следующих принципов: обозримости («организованности») и прозрачности культурного ландшафта государства; единства и совместимости элементов информационной инфраструктуры сохранения культурного наследия; социально-культурного мониторинга (на основе полисистемного подхода); ситуационного анализа и реагирования; стратегической ориентации; ускоренной адаптации культурных практик и человеческого капитала (информатизация профессиональной структуры, маркетинг цифровых решений и массовые цифровые компетенции).

Принципы эффективности проектов цифровизации определяют целесообразность инвестиций в цифровизацию сохранения культурного наследия:

1. Принцип надежности информационных систем сохранения культурного наследия.
2. Принцип результативности предполагает многоуровневое понимание эффективности и выработку критериев результативности упреждения рисков внешней и внутренней опасности для объектов культурного наследия как ключевой цели, критериев результативности (KPI) как метрики мониторинга состояния и прогресса достижения целей сохранения культурного наследия для своевременной коррекции методического обеспечения социальной эффективности.
3. Принципы достоверности, оперативности, полноты. Достоверность предполагает снижение ошибок в показателях функционального соответствия, выявленных в ходе эксплуатации цифровых решений и построенных на их основе информационных систем. Оперативность должна сокращать времена реагирования на выявленные риски различных опасностей физического или социального разрушения, культурной маргинализации объектов культурного наследия. Полнота предполагает получение необходимой пертинентной информации вне дополнительных запросов со стороны специалиста, достаточной, а в ряде случаев и избыточной для принятия решений в процессах сохранения культурного наследия.
4. Принцип разумной конфиденциальности предполагает оценку ряда социальных рисков и выработку системы противодействия им посредством ограничения доступа к информационным системам сохранения культурного наследия.
5. Принцип функциональной адекватности – информационные системы должны быть адекватны сложности объектов культурного наследия, а также культурных процессов в контексте их отражения в компьютерных моделях (сочетание частных и системных моделей).
6. Принцип отраслевой персонализации предполагает возможность самостоятельного использования ИТ-решения функциональным и отраслевым специалистом (экспертом, музеологом, исследователем и т. д.). Реализация этого принципа предполагает, во-первых, тесный контакт информационного и отраслевого специалистов при разработке цифровых решений и усиление информационной подготовки специалистов в сфере культуры как условия этого контакта; во-вторых, управление информационным рынком в русле ценовой доступности новых ИТ-решений для сферы культуры.

Заключение

Таким образом, современное общество выстраивает новую парадигму управления культурой, в которой цифровизация сохранения культурного наследия – одна из приоритетных задач. Цифровизация культурного наследия – это совокупность новых ИТ-решений, нового дизайна информационного пространства культуры, новых отношений в профессиональной и социальной среде, новых экономических моделей. Между тем изучение публикационного потока и потока регистрируемых результатов интеллектуальной деятельности не позволяет говорить об интенсивных и эффективных исследованиях и разработках, направленных на создание новых цифровых инструментов сохранения культурного наследия. И цель этой статьи – привлечь внимание молодых исследователей в области прикладной информатики в культуре, в области цифровой гуманитаристики (Digital Humanities) к актуальной и интересной научной и практической задаче.

Литература

Войтин, Тютюнник 2014 – *Войтин А.О., Тютюнник В.М.* Новые подходы к сохранению и актуализации культурного наследия // В мире научных открытий. 2014. № 4 (52). С. 37–44.

Лопатина, Неретин 2018 – Лопатина Н.В., Неретин О.П. Сохранение цифрового культурного наследия в едином электронном пространстве знаний // Вестник Московского государственного университета культуры и искусств. 2018. № 5 (85). С. 74–80.

Неретин 2015 – *Неретин О.П.* Формирование механизма взаимодействия групп поддержки в системе стратегического управления учреждениями культуры: Автореферат дис. ... д-ра эконом. наук. СПб., 2015. 22 с.

Неретин 2018 – *Неретин О.П.* Интеллектуальная собственность как инструмент цифровизации культуры: к вопросу сохранения традиционных знаний и традиционных выражений культуры // Вестник Московского государственного университета культуры и искусств. 2018. № 6 (86). С. 158–163.

Поппер 2002 – *Поппер К.Р.* Объективное знание. Эволюционный подход. М.: Эдиториал УРСС, 2002.

Сляднева 1999 – *Сляднева Н.А.* Homo informaticus – человек эпохи информатизации// Научно-техническая информация. Сер. 1. 1999. № 3. С. 9–13

Тютюнник, Войтин, Тявкин 2016 – *Тютюнник В.М., Войтин А.О., Тявкин И.В.* Организационно-технологический механизм сохранения и виртуализации объектов материального наследия культуры // Глобальный научный потенциал. 2016. № 7 (64). С. 41–49.

Ярилова 2008 – *Ярилова О.С.* О концепции сохранения и развития нематериального культурного наследия народов Российской Федерации // Вестник Российской нации. 2008. № 1 (1). С. 237–239.

References

Lopatina, N.V. and Neretin, O.P. (2018), "Preservation of digital cultural heritage in the unified electronic space of knowledge", *Bulletin of the Moscow State University of Culture and Arts*, vol. 5 (85), pp. 74–80.

Neretin, O.P. (2015), *Forming the interaction mechanism of the support groups for the strategic management system of cultural institutions* [Formirovanie mekhanizma vzaimodeistviya grupp podderzhki v sisteme strategicheskogo upravleniya uchrezhdeniyami kul'tury], Abstract of D. Sc. dissertation, Saint Petersburg, Russia.

Neretin, O.P. (2018) "Intellectual property as a tool for digitalization of culture. On the issue of preserving traditional knowledge and traditional expressions of culture", *Bulletin of the Moscow State University of Culture and Arts,* vol. 6 (86), pp. 158–163.

Popper, K.R. (2002), *Ob'ektivnoe znanie. Evoluzionniy podhod* [Objective knowledge. Evolutionary approach], Editorial URSS, Moscow, Russia.

Slyadneva, N.A. (1999), "Homo informaticus – man of the era of Informatization", *Scientific and technical information. Series 1*, vol. 3, p. 9–13.

Tyutyunnik, V.M., Voitin, A.O. and Tyavkin, I.V. (2016), "Organizational and technological mechanism for the preservation and virtualization of objects in the material culture heritage" *Global scientific potential*, vol. 7 (64), pp. 41–49.

Voitin, A.O. and Tyutyunnik, V.M. (2014), "New approaches to the preservation of cultural heritage and its updating", *In the World of Scientific Discovery*, vol. 4 (52), pp. 37–44.

Yarilova, O.S. (2008), "On the concept of preserving and developing the intangible cultural heritage of the peoples of the Russian Federation" *Bulletin of the Russian Nation*, vol. 1 (1). pp. 237–239.

Информация об авторе

Наталья В. Лопатина, доктор педагогических наук, профессор, Московский государственный институт культуры, Москва, Россия; 141406, Россия, Московская обл., Химки, ул. Библиотечная, 7; dreitser@yandex.ru

Information about the author

Natalia V. Lopatina, Dr. of Sci. (Education), professor, Moscow State Institute of Culture, Moscow, Russia; bld. 7, Bibliotechnaya Str., Khimki, Moscow Region, Russia, 141406; dreitser@yandex.ru

УДК 004.056
DOI: 10.28995/2686-679X-2020-4-19-30

Обеспечение информационной безопасности детей в Российской Федерации

Людмила А. Наумова
Московский государственный лингвистический университет, Москва, Россия, lyudmila101202@yandex.ru

Дмитрий Н. Баранников
Московский государственный лингвистический университет, Москва, Россия; Российский государственный гуманитарный университет, Москва, Россия, d.2006@mail.ru

Дмитрий А. Митюшин
Российский государственный гуманитарный университет, Москва, Россия, dalexx@inbox.ru

Аннотация. Одной из положительных сторон достижений XXI в. является доступность разнообразной информации. Любой человек, имеющий доступ к сети Интернет с помощью технических устройств осуществляет «вход в информационное пространство». С использованием сети Интернет (информационных технологий) можно не только воспользоваться электронной библиотекой, расширяя свой кругозор энциклопедическими знаниями, но и осуществлять образовательную деятельность и обмениваться любой информацией. Однако личность с неокрепшей психикой получает доступ к информации, не соответствующей возрастной категории. Проблема доступа детей к информации, имеющей возрастные ограничения, обсуждается, и принимаются решения, законодательно регулирующие отношения будущих эрудитов с информацией, размещенной в открытом доступе. В обществе существует неоднозначность формулировок и взглядов на информацию, имеющую возрастные ограничения. Такая неоднозначность приводит к тому, что подрастающее поколение не защищено от информации, доступ к которой им ограничен. Поэтому, сосредоточив регулирующие функции в одном органе исполнительной власти, можно достичь должного уровня защиты от информации, имеющей возрастные ограничения. Эти функции можно было бы придать

такому органу исполнительной власти, как Министерство просвещения Российской Федерации.

Ключевые слова: информация, безопасность, защита детей, Женевская декларация, нравственность, телевещание, школьная программа, Интернет

Для цитирования: Наумова Л.А., Баранников Д.Н. Митюшин Д.А., Обеспечение информационной безопасности детей в Российской Федерации // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2020. № 4. С. 19–30. DOI: 10.28995/2686-679X-2020-4-19-30

Ensuring information security of children in the Russian Federation

Lyudmila A. Naumova

Moscow State Linguistic University, Moscow, Russia, lyudmila101202@yandex.ru

Dmitrii N. Barannikov

Moscow State Linguistic University, Moscow, Russia; Russian State University for the Humanities, Moscow, Russia, d.2006@mail.ru

Dmitrii A. Mityushin

Russian State University for the Humanities, Moscow, Russia, dalexx@inbox.ru

Abstract. One of the positive aspects of the achievements in the 21st century is the information variety availability. Any person who has access to the Internet by the technical devices enters the information space. Using the Internet (information technology) any person can not only obtain the electronic library thus expanding one's horizons with encyclopedic knowledge, but also carry out educational activities and share any information. However, a person with a fragile psyche gets access to information that does not correspond to the age category. An issue of children's access to information that has age restrictions is discussed, and decisions are made that regulate by law the relationship of future erudites with information posted in the public domain. In society there is ambiguity in the formulation and views on information that has age restrictions. Such an ambiguity leads to the fact that the younger generation is not protected from the information an access to which is restricted to them. Therefore, by concentrating regulatory functions in one executive body, it is possible to achieve the proper level of protection against information that has age restrictions. Those functions could be assigned to such an executive body as the Russian Federation Ministry of Education.

Keywords: information, safety, child protection, Geneva Declaration, morality, television broadcasting, school curriculum, Internet

For citation: Naumova, L.A., Barannikov, D.N. and Mityushin, D.A. (2020), "Ensuring cybersecurity of children in the Russian Federation", *RSUH/RGGU Bulletin. "Information Science. Information Security. Mathematics" Series*, no. 4, pp. 19–30, DOI: 10.28995/2686-679X-2020-4-19-30

Введение

Во все времена самым уязвимым звеном общества были дети. Поэтому неоднократно возникал вопрос о рассмотрении ребенка как самостоятельной личности со своими правами, а не только обязанностями. Эглантин Джебб смогла обратить внимание на социальные проблемы детей, разработала их права и оформила юридическим актом.

Впервые в ноябре 1924 г. на пятой Ассамблее Лиги Наций в Женеве был рассмотрен и принят такой нормативный акт, который впоследствии назвали Женевская декларация. Для того времени было обычным делом привлекать к труду несовершеннолетних, заниматься их продажей и использовать для проституции. Данной Декларацией запрещалось привлекать несовершеннолетних к оказанию услуг сексуального характера, а также пресекались любые попытки торговли людьми. Принятие этого документа явилось прорывным событием, т. к. обозначились права несовершеннолетних, которые надлежало защищать. Шло время, Декларация дополнялась новыми пунктами, но проблема защиты детей остается актуальной и в современном мире.

Обеспечение информационной безопасности детей в Российской Федерации

В 2003 г. в Женевской декларации принципов была сформирована одна из главных тенденций развития стран в XXI в.: «Построение информационного общества – глобальная задача в новом тысячелетии». Принимая во внимание все стоящее перед современным мировым сообществом, Россия не только уделяет внимание созданию информационного сообщества, но и выделяет сферу обеспечения безопасности функционирования общественной жизни в современных условиях. Исходя из проведенного анализа, одной из основных угроз для населения России является оказание информационно-психологического воздействия с целью размывания традиционных российских духовно-нравственных

ценностей[1]. Наиболее уязвимыми для такого воздействия оказались молодые люди возрастной категории до 18 лет. Для снижения и предотвращения вышеизложенной угрозы был принят ряд федеральных законов, одним из которых является Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» от 29.12.2010 г. № 436-ФЗ (далее – закон).

Закон направлен на обеспечение защиты подрастающего поколения и предотвращение травмирующего информационного воздействия на психику общества. Одной из достигаемых законом задач является информационная безопасность детей – состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию. В действующем нормативно-правовом акте определяются запрещенные для распространения среди детей виды информации, такие как активизирующие к действиям, угрожающим жизни и здоровью, самоубийству, употреблению запрещенных веществ, табачной, алкогольной и иной продукции, участию в азартных играх и других.

Кроме того, обращается пристальное внимание на информацию, распространение которой ограничено среди детей определенных возрастных категорий.

В статье 12 закона прописаны требования классификации информационной продукции с обозначающими ее знаками. Также в законе обозначены возрастные ограничения, статьи, устанавливающие и регулирующие каждый вид информационной продукции:

Статья 7. Для детей, не достигших возраста шести лет, – в виде цифры «0» и знака «плюс»;

Статья 8. Для детей, достигших возраста шести лет, – в виде цифры «6» и знака «плюс» и (или) текстового предупреждения в виде словосочетания «для детей старше шести лет»;

Статья 8. Для детей, достигших возраста двенадцати лет, – в виде цифры «12» и знака «плюс» и (или) текстового предупреждения в виде словосочетания «для детей старше 12 лет»;

Статья 9. Для детей, достигших возраста шестнадцати лет, – в виде цифры «16» и знака «плюс» и (или) текстового предупреждения в виде словосочетания «для детей старше 16 лет»;

Статья 10. Запрещенная для детей, – в виде цифры «18» и знака «плюс» и (или) текстового предупреждения в виде словосочетания «запрещено для детей».

---

[1] Указ Президента Российской Федерации «Об утверждении Доктрины информационной безопасности Российской Федерации» от 05.12.2016 г. № 646 [Электронный ресурс] // Правительство РФ. URL: http://www.kremlin.ru/acts/bank/41460/page/1 (дата обращения 9 ноября 2020).

Кроме того, закон обязал производителей, распространителей информационной продукции предупреждать о ее возрастных ограничениях перед началом демонстрации при кино- и видеообслуживании, при этом размер знака информационной продукции должен занимать не менее 5% площади афиши, объявления, а также входного билета и других документов.

Существуют и дополнительные требования к распространению информации посредством теле- и радиовещания. Информация, запрещенная для распространения среди детей, не подлежит показу и трансляции с 4 часов до 23 часов по местному времени, а информационная продукция для детей, достигших возраста шестнадцати лет, – с 7 часов до 21 часа по местному времени. Также телевизионное вещание обязательно должно сопровождаться в начале и возобновлении трансляции демонстрацией знака информационной продукции, а при радиовещании – сообщением о возрастном ограничении распространения информации. Ответственность за правонарушения законодательства РФ о защите детей от информации назначается в соответствии с законодательством РФ[2].

Контрольные функции за соблюдением правовых положений по защите детей от информации, причиняющей вред их здоровью и (или) развитию, осуществляет федеральный орган исполнительной власти по контролю и надзору в сфере СМИ, в области защиты прав потребителей и в сфере образования и науки. Не исключается в данной области и общественный контроль.

Однако общественность неоднозначно отнеслась к закону и подвергла критике некоторые его положения. По данным, размещенным в СМИ, сообщается, что под запрет попадут общеизвестные советские мультфильмы. Исключая неоднозначное толкование положений закона, руководитель Роскомнадзора Александр Жаров в интервью «Российской газете» сообщил: «Позиция Роскомнадзора выражена достаточно четко. Публично она была озвучена вчера на совещании с печатными СМИ и сетевыми изданиями: мультфильм Ну, погоди! и вся подобного рода продукция является культурной ценностью для нашей страны, а потому нет никакой необходимости ограничивать показ, маркировать эту продукцию»[3]. Следует отметить, что несмотря на вышеизложенное

---

[2] Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» от 29.12.2010 г. № 436-ФЗ. [Электронный ресурс] // Правительство РФ. URL: http://www.kremlin.ru/acts/bank/32492/page/1 (дата обращения 4 ноября 2020).

[3] *Шадрина Т.* Ну, погодите! Ну, послушайте [Электронный ресурс] // Российская газета – Федеральный выпуск, № 200 (5873). URL: https://rg.ru/2012/08/31/zharov.html (дата обращения 14 ноября 2020).

комментирование распространители данного вида информационной продукции алогично маркируют мультфильмы. На сегодняшний день известно о запрете показа «Ну, погоди!», «Бременские музыканты» из-за «действий, побуждающих детей к употреблению табачных изделий, бродяжничеству и т.д.», однако точного регулирования данного вопроса нет. В то же время иностранные мультфильмы буквально наводнили российские телеканалы. Почему же не запретят «Том и Джерри» с возрастным ограничением «0+», где напрямую транслируются насилие и безнаказанность? Или «Губка Боб Квадратные Штаны» – «0+» с последующим изображением негативных персонажей: не желающих взрослеть, алчных героев, без последующей победы добра над злом? Из-за различий западной и российской культур следует регулировать в первую очередь поступление иностранной информационной продукции.

К сожалению, разногласия в подходе сохранились из-за иногда абсурдной правоприменительной практики. Они проявились во внесении в 2019 г. депутатами Е.А. Ямпольской, А.М. Шолоховым и другими в Государственную Думу Законопроекта № 717228-7[4]. Авторы обосновывали необходимость принятия изменений «учащением случаев неоднозначного и абсурдного правоприменения», «разной трактовкой возрастных ограничений производителями для произведений литературы и искусства», «негативным отражением обязательной классификации на книготорговле и взаимодействии детей и подростков с бумажной книгой». Законопроект предлагал признание преимущественного права детей на доступ к культурным ценностям; изменение основных правовых механизмов, регулирующих доступ детей к информационной продукции; кардинальное изменение возрастной классификации и маркировки информационной продукции на текстовые предупреждения, выраженные словосочетаниями «для семейного чтения», «для семейного просмотра» и т. д.; сохранение единственной категории «18+» и другие положения.

В тоже время в Конституции РФ п. 3 ст. 55[5] указана о возможность ограничения прав и свобод человека и гражданина в целях

[4] Законопроект «О внесении изменений в статью 30 Закона Российской Федерации «Основы законодательства Российской Федерации о культуре» и отдельные законодательные акты Российской Федерации в связи с совершенствованием законодательных механизмов, регулирующих доступ детей к культурным ценностям и культурным благам» № 717228-7 [Электронный ресурс] // СОЗД ГАС «Законотворчество». URL: https://sozd.duma.gov.ru/bill/717228-7 (дата обращения 9 ноября 2020).

[5] Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ

защиты нравственности, здоровья, прав и законных интересов, что пересекается со ст. 9 Федерального закона «Об информации, информационных технологиях и о защите информации»[6]. Таким образом, правомерность ограничения свободы получения информации и доступа к ней детей в целях обеспечения всесторонней защиты детей влечет возможность и законность такого ограничения в отношении доступа детей к культурным ценностям, представленным в виде информационной продукции.

В Заключении, представленном В.В. Абраменковой, В.Г. Елизаровым и другими, были сделаны следующие выводы о предложенном законопроекте:

предлагаемые законопроектом изменения противоречат целям и задачам государственной политики Российской Федерации в сфере информационной безопасности детей;

концепция законопроекта противоречит общепризнанному принципу преимущественного права родителей на обучение и воспитание своих детей перед всеми другими лицами;

законопроект разработан с игнорированием общепринятого возрастно-психологического подхода к оценке вредного воздействия информационной продукции на психическое развитие, здоровье и психологическое благополучие детей;

предусмотренная законопроектом отмена большинства действующих правовых гарантий информационной безопасности детей в области культуры противоречит национальным интересам, стратегическим целям и задачам Российской Федерации[7].

Несмотря на данное заключение законопроект был принят в первом чтении 05.12.2019 г., однако с того периода развития законодательный процесс не имеет.

Одним из существенных недостатков является исключение из сферы действия закона в п. 3 ч.2. ст. 1 оборота информационной продукции, имеющей значительную историческую, художественную или иную культурную ценность для общества. Закон не дает

о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 01.07.2020 № 11-ФКЗ) [Электронный ресурс] // Государственная Дума РФ. URL: http://duma.gov.ru/news/48953/ (дата обращения 10 ноября 2020).

[6] Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 г. № 149-ФЗ [Электронный ресурс] // Правительство РФ. URL: http://www.kremlin.ru/acts/bank/24157 (дата обращения 7 ноября 2020).

[7] Заключение на проект Федерального закона № 717228-7 [Электронный ресурс]. URL: https://regnum.ru/uploads/docs/2019/10/24/regnum_file_1571915081469535.pdf (дата обращения 9 ноября 2020).

определение или критерии данного вида информации. В связи с тем что производители, распространители информационной продукции обязаны самостоятельно регулировать возрастную маркировку товара, отсутствие единого списка маркировки привело к дифференциации отнесения одного и того же вида информации к возрастным категориям. Например, произведение И.А. Бунина «Легкое дыхание» редакторы известных книжных интернет-магазинов «ЛитРес», «Livelib», «ЧитайГород» относят как «6+», «12+», «16+» соответственно. Данная неточность касается и произведений классической литературы: распространители информационной продукции маркируют «Войну и мир» Л.Н. Толстого «12+», «16+». Однако данный роман может вполне быть причислен и к информации, имеющей значительную культурную ценность для общества, по причине чего иногда его не относят ни к одной возрастной категории, например, издательство «Азбука».

Общественные прения и здравый смысл повлияли на доработку закона и вступили в силу 29.10.2019 г. изменения в Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию»:

был добавлен п. 3.1 ч. 2 ст. 5 вид информации, запрещенной для распространения среди детей, содержащей изображение или описание сексуального насилия;

в ч. 7.1. ст. 11 организатор зрелищного мероприятия обязан не допускать на мероприятие, содержащее информацию, запрещенную для распространения среди детей лиц, не достигших восемнадцатилетнего возраста, а контролирующий проход вправе потребовать у посетителя документ, удостоверяющий личность;

п. 4–5 ст. 16 не допускает распространение инфопродукции «18+» на расстоянии менее чем сто метров по прямой линии без учета искусственных и естественных преград от ближайшей точки, граничащей с территорией организации;

согласно ч. 9 ст. 16 при размещении анонсов фильмов, содержащих информацию, запрещенную для распространения среди детей в соответствии с настоящим Федеральным законом, не допускается использование фрагментов указанных фильмов, содержащих информацию, запрещенную для распространения среди детей;

часть 6 ст. 11 данного закона закрепляет правило о том, что продажа, прокат, аренда, а также выдача из фондов общедоступных библиотек информационной продукции лицам, не достигшим восемнадцатилетнего возраста, не допускается[8].

[8] *Григорьев Д.* Обзор изменений в Закон о защите детей от негативной информации. [Электронный ресурс] // Издательская группа «Закон». URL:

Как было сказано выше, так как не существует единого списка маркировки, то в фондах общедоступных библиотек могут находиться одни и те же произведения разных изданий, а следовательно, разных возрастных категорий. А некоторые произведения школьной программы, обязательные для изучения, например «Тихий Дон» М.А. Шолохова имеют возрастное ограничение «18+», что не позволяет большинству обучающихся 10–11 классов изучить данный роман. Приведенные примеры показывают наличие противоречий в рассматриваемом законе.

Еще одним недостатком данного Федерального закона, отрицательно влияющим на идеологическое восприятие, является несовпадающая с иностранной киноиндустрией возрастная классификация. Выше уже была изложена возрастная категория российской системы, однако она заметно отличается от рейтинга MPAA (Системы рейтингов Американской киноассоциации), содержащего следующее разделение:

1) рейтинг G – видеопродукция без ограничений;
2) рейтинг PG – фильм для просмотра с родителями;
3) рейтинг PG-13 – детям до 13 лет разрешен просмотр в сопровождении родителей (одного родителя);
4) рейтинг R – подростки до 17 лет допускаются на фильм только в сопровождении одного из родителей, либо законного представителя;
5) рейтинг NC-17 – настоятельно не рекомендуется просмотр зрителям моложе 17 лет, тем не менее в сопровождении родителей зрители допускаются[9].

Однако если в российской системе возрастного ограничения в статьях 7–10 ясно указаны признаки отнесения информационной продукции к данному виду категории, то в американской это представлено расплывчато. Важно отметить, что в MPAA именно родитель регулирует просмотр информационной продукции своего ребенка, у нас же данная функция возложена на коммерческие организации в сфере производства и распространения информационного оборота. Кроме того, наши государства имеют разные уникальные культуры, что также является сложностью при маркировке продукции иностранной киноиндустрии. К фильмам категории «16+» в настоящее время относятся такие, как: «Взрослые игры», США, 2017 г. (начинается с провокационной сцены, в которой

---

https://zakon.ru/blog/2019/11/19/obzor_izmenenij_v_zakon_o_zaschite_detej_ot_negativnoj_informacii (дата обращения 18 ноября 2020).

[9] *Юсев А.* Сравнение российского и американского подходов к возрастным ограничениям в кино [Электронный ресурс]. URL: https://yusev-alexei.livejournal.com/169188.html (дата обращения 19 ноября 2020).

главная героиня – циничная семнадцатилетняя девушка, не обремененная моральными принципами и идеалами, вступает в сексуальный контакт с полицейским, пока две ее подруги снимают это на видео с целью последующего шантажа и вымогательства); «Мечты сбываются», США, 2009 г. (молодежная комедия про двоих друзей, попавших в фантастическую вселенную, где все их интимные мечты могут сбыться); «Сексуальное настроение», Испания, 2005 г. (раскованная комедия положений о парне из провинции, покоряющем столицу Испании через отрасль эскорт-услуг); «Смертный приговор», США, 2007 г. (триллер-боевик о превращении менеджера крупной компании, обходительного и вежливого человека с репутацией отличного семьянина, в профессионального убийцу). Если в США считается нормой просмотр приведенных фильмов зрителями младше 18-ти лет, то попадая в кинопрокат России, они должны быть рассмотрены в российской системе возрастных ограничений.

В современных условиях создания информационного сообщества государство обязано обеспечить безопасное функционирование общества, а особенно наиболее социально восприимчивой группы населения – молодого поколения. С развитием информационных технологий человек получает огромное количество информации, которую сложно контролировать и отфильтровывать даже взрослому человеку. Поэтому необходимо повысить правовые гарантии обеспечения информационной безопасности и привести к снижению негативных процессов растления, виктимизации, криминализации и маргинализации несовершеннолетнего населения России. Очевидное значение имеет законодательство в сфере обеспечения защиты детей от информации, и в частности Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию». Однако данный нормативно-правовой акт имеет ряд недоработок: неточность понятия «информация, имеющая значительную историческую, художественную и иную культурную ценность», отсутствие единого реестра маркировки информационной продукции, соотношение систематизаций российских и иностранных возрастных ограничений. Кроме того, он лишь устанавливает требования регулирования данных отношений. Основную и важную функцию выполняют коммерческие организации, а государство вмешивается во время спорных моментов. То есть прямое государственное регламентирование отсутствует. Таким образом, для устранения утечки информации, причиняющей вред здоровью и (или) развитию детей, необходимо пересмотреть некоторые пункты рассмотренного закона.

Заключение

Федеральный закон от 29.12.2010 №436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» должен учитывать, что дети в, основном, с 3-4 лет начинают посещать общественные учреждения для воспитания и образования: детские сады, в дальнейшем школы, колледжи или вузы [Александрова 2018]. Весь этот период ребенок не только познает окружающий мир, но и приобретает важные знания, которыми пополняется его багаж для личностного становления и использования в практической деятельности. Период становления личности является важным периодом в жизни человека, поэтому его необходимо контролировать и регулировать на федеральном уровне. То есть именно Министерствам просвещения, науки и образования необходимо подвергать ревизии поступающий поток информации. Разумеется, нельзя отрицать воздействие других сфер деятельности общества, где пребывает ребенок [Поклонцев 2018], однако в образовательных учреждениях должна также присутствовать воспитательная функция. Особенно в раннем возрасте эти важные социальные институты должны прививать и развивать внутренний стержень детей. Это станет первым этапом предотвращения негативного информационного влияния, так как дети будут психологически и морально устойчивы к внешнему информационному воздействию.

Литература

Александрова 2018 – *Александрова М. Ю.* Правовое регулирование информационной безопасности образовательной организации // Молодой ученый. 2018. № 7 (193). С. 123–124.

Поклонцев 2018 – *Поклонцев К. В.* Правовая защита несовершеннолетних от информации, причиняющей вред их здоровью и развитию, на примере социальной сети «ВКонтакте» // Молодой ученый. 2018. № 47 (233). С. 142–144.

References

Aleksandrova, M.Yu. (2018), “Legal regulation of the information security for educational organization”, *Molodoi uchenyi,* no. 7 (193), pp. 123–124.

Poklontsev, K.V. (2018), “Legal protection of minors from information harmful to their health and development, by the example of the social network “Vkontakte””, *Molodoi uchenyi,* no. 47 (233), pp. 142–144.

Информация об авторах

Людмила А. Наумова, студент, Московский государственный лингвистический университет, Москва, Россия; 119034, Россия, Москва, ул. Остоженка, д. 38, стр. 1; lyudmila101202@yandex.ru

Дмитрий Н. Баранников, кандидат военных наук, Московский государственный лингвистический университет, Москва, Россия; 119034, Россия, Москва, ул. Остоженка, д. 38, стр. 1;

Российский государственный гуманитарный университет, Москва, Россия; 125993, Россия, Москва, Миусская площадь, д. 6; d.2006@mail.ru

Дмитрий А. Митюшин, кандидат технических наук, Российский государственный гуманитарный университет, Москва, Россия; 125993, Россия, Москва, Миусская пл., д. 6; dalexx@inbox.ru

Information about the authors

Lyudmila A. Naumova, student, Moscow State Linguistic University, Moscow, Russia; bld. 38, Ostozhenka Str., Moscow, Russia, 119034; lyudmila101202@yandex.ru

Dmitrii N. Barannikov, Cand. of Sci. (Military), Moscow State Linguistic University, Moscow, Russia; bld. 38, Ostozhenka Str., Moscow, Russia, 119034;

Russian State University for the Humanities, Moscow, Russia; bld. 6, Miusskaya Sq., Moscow, Russia, 125993; d.2006@mail.ru

Dmitrii A. Mityushin, Cand. of Sci. (Engineering), Russian State University for the Humanities, Moscow, Russia; bld. 6, Miusskaya Sq., Moscow, Russia, 125993; dalexx@inbox.ru

УДК 004.056
DOI: 10.28995/2686-679X-2020-4-31-45

Сравнительный анализ результативности и востребованности итогов научной деятельности российских ученых по актуальным направлениям исследований в области информационной безопасности

Валерий В. Арутюнов

Российский государственный гуманитарный университет, Москва, Россия, warut698@yandex.ru

Аннотация. В статье отмечается повышение в XXI в. значимости обеспечения информационной безопасности предприятий при обработке, хранении, поиске и передаче информации в информационных системах и информационно-телекоммуникационных сетях. Рассматриваются актуальные направления исследований в области информационной безопасности (ИБ), в число которых входят биометрические методы и средства защиты информации, технология блокчейн, криптография (включая квантовую криптографию), системы обнаружения вторжений (IDS-системы), стеганографические методы защиты информации, системы предотвращения утечки информации (DLP-системы), кибербуллинг, методы обфускации, управление ИБ. Проанализирована динамика изменения наукометрических показателей научной деятельности (публикационной активности, цитируемости и индекса Хирша) в 2010–2019 гг. для данных научных направлений. Выявлен ряд закономерностей этих показателей за анализируемый период, включая взрывной рост публикаций для следующих направлений: технология блокчейн, управление ИБ, биометрические методы и средства защиты информации, квантовая криптография, методы обфускации. После четырехлетней стабильной востребованности итогов исследований в области управления ИБ с 2015 г. наблюдается падение этого показателя, вызванного, возможно, кризисом 2014 г.

Рост индекса цитирования до конца анализируемого периода отмечался лишь для двух направлений: технологии блокчейн и кибербуллинга. Максимум показателей востребованности итогов работ российских ученых, достигнутый российскими учеными, был выявлен в области кибербуллинга, минимум – в сфере DLP-систем.

Анализ годовых наукометрических показателей осуществлялся с использованием базы РИНЦ (Российского индекса научного цитирования).

Ключевые слова: информационная безопасность, наукометрические показатели, публикационная активность, индекс Хирша, цитируемость, актуальные направления исследований, результативность научной деятельности

Для цитирования: Арутюнов В.В. Сравнительный анализ результативности и востребованности итогов научных исследований российских ученых по актуальным направлениям в области информационной безопасности // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2020. № 4. С. 31–45. DOI: 10.28995/2686-679X-2020-4-31-45

Comparative analysis in the effectiveness and relevance of the scientific working results of Russian scientists in current areas of research in the field of the information security

Valery V. Arutyunov

Russian State University for the Humanities, Moscow, Russia, warut698@yandex.ru

Abstract. The article notes the increasing importance of ensuring information security in the data processing, storage, search and transmission in the information systems and information and telecommunications networks in the 21st century. Current research areas in the field of the information security are considered, such as biometric methods and the information protection tools, blockchain technology, cryptography (including quantum cryptography), Intrusion Detection Systems (IDS), the steganographic information protection methods, Data Leakage Prevention systems (DLP-systems), cyberbullying, obfuscation methods, and the information security management. The author analyzes the dynamics of changes in scientometric indicators for scientific activity (publication, citation and Hirsh index) in 2010-2019 with relation to the research areas concerned. A number of trends for those indicators were revealed during the analyzed period, including an explosive growth of publications in the following areas: blockchain technology, information security management, biometric methods and the information protection tools, quantum cryptography, obfuscation methods. After four years of stable demand for research results in the field of information security management, since 2015, that indicator has been falling, what was possibly caused by the 2014 crisis.

The growth of the citation index until the end of the period was noted only for two areas: blockchain technology and cyberbullying. The maximum value in indicators of demand for the results of Russian scientists work, achieved by

Russian scientists in 2010-2019, was identified in the area of cyberbullying, the minimum – in the field of DLP-systems. The analysis of annual scientometric indicators was carried out using the RSCI database (Russian science citation index).

Keywords: information security, scientometric indicators, publication activity, h-index, citation, current research directions, scientific performance

For citation: Arutyunov, V.V. (2020), "Comparative analysis in the effectiveness and relevance of the scientific working results of Russian scientists in current areas of research in the field of the information security", *RSUH/RGGU Bulletin. "Information Science. Information Security. Mathematics" Series*, no. 4, pp. 31–45, DOI: 10.28995/2686-679X-2020-4-31-45

Введение

Начало XXI века характеризуется наличием в России большого числа многофункциональных информационных систем (ИС) и информационно-телекоммуникационных сетей (ИТС) высокой степени интеграции, использующих последние достижения в развитии технологии обработки, хранения, поиска и передачи информации. При этом в наши дни повышается значимость оперативного и профессионального решения вопросов информационной безопасности (ИБ) предприятий и организаций с целью создания основы для бесперебойного функционирования значительного числа ИС и ИТС в стране, обеспечивающих штатную реализацию автоматизированных производственных и научных процессов [Арутюнов 2013]. В работе [Арутюнов 2020] отмечается рост публикационной активности в России в сфере ИБ: количество публикаций в 2018 г. в этой области исследований увеличилось практически втрое по сравнению с 2012 г.

О повышенном внимании руководителей и специалистов предприятий к вопросам обеспечения ИБ в XXI в. свидетельствует и тот факт, что в конце первого десятилетия XXI в. в Государственный рубрикатор научно-технической информации России была введена новая рубрика: 81.93.29 – Информационная безопасность. Защита информации. Еще одним свидетельством, подтверждающим пристальное внимание государственных и коммерческих организаций к вопросам защиты информации, циркулирующей в сети Интернет, является превышение в 2017 г. объема зашифрованного трафика в Интернете по сравнению с общедоступным.

Поэтому вполне естественным представляется тот факт, что во многих вузах страны (в том числе в РГГУ) с начала второго десятилетия XXI в. студентам преподается дисциплина, рассматрива-

ющая основные актуальные тенденции исследований в области защиты информации.

К числу таких актуальных направлений исследований в области ИБ можно отнести следующие:

- биометрические методы и средства защиты информации;
- кибербуллинг (преднамеренные агрессивные действия с целью нанесения как минимум психологического вреда человеку, осуществляемые с использованием электронной почты, мобильной связи, а также в социальных сетях и на web-сайтах);
- криптография (включая квантовую криптографию);
- методы обфускации;
- системы обнаружения вторжений (IDS-системы);
- системы предотвращения утечки информации (DLP-системы);
- стеганографические методы защиты информации;
- технология блокчейн;
- управление ИБ.

В связи с изложенным возникает вопрос о количественной оценке результативности и востребованности итогов работ российских ученых в XXI в. в указанных областях ИБ. Отметим, что российские исследователи в области ИБ входят в состав более чем четырехсоттысячной исследовательской армии страны [Ширяев, Доронина 2019], значительное их количество, наряду с другими, интересует естественный вопрос: как научное сообщество (отечественное или мировое) оценивает результаты их научной деятельности.

Наукометрические показатели научной деятельности российских ученых по актуальным направлениям исследований в области информационной безопасности

В XXI в. в мире и России все в большей степени оценивают итоги работы ученых и специалистов в различных сферах науки и техники по конкретным количественным результатам, базирующимся на наукометрических показателях их научной деятельности (публикационной активности P, цитируемости C и индексе Хирша H) [Арутюнов 2009; Арутюнов 2015; Арутюнов, Цветкова 2018; Донгак, Шатохин, Мещеряков 2019; Молчанова, Сканцев, Спасенников 2019; Grinev 2019].

В России в последние годы указанные показатели активно используются для оценки результатов научной деятельности вузов и научных организаций страны.

При этом в наши дни значительный интерес представляют не только опубликованные итоги исследований, но и востребован-

ность V научным сообществом и специалистами результатов научной деятельности ученых по различным направлениям наук, определяемая соотношением C / P.

Ниже приводятся результаты анализа динамики публикационной активности, цитируемости и индекса Хирша российских ученых за последнее десятилетие (2010-2019 гг.), а также востребованность итогов исследований в вышеуказанных областях ИБ, которые отражаются в соответствующих публикациях.

Показатели были получены в основном по данным из созданной в Научной электронной библиотеке России базы данных РИНЦ (Российского индекса научного цитирования) [РИНЦ 2020], где формируются данные о публикационной активности и цитируемости ученых и организаций – в основном из России и в меньшей степени – из стран СНГ.

Для примера, на рис. 1 и 2 представлена динамика публикационной активности и цитируемости российских ученых в 2010–2019 гг. в области управления ИБ и квантовой криптографии. Для обоих направлений наблюдался рост числа публикаций практически до конца исследуемого периода, что объясняется все возрастающим интересом исследователей к итогам работ в этих областях. При этом если максимум публикаций в области управления ИБ превышал минимум 2012 г. в шесть раз, то максимум публикаций в области квантовой криптографии был практически в пять раз больше минимума 2012 г. В то же время максимум цитируемости в сфере управления ИБ отмечался уже в 2015 г., а в области квантовой криптографии – еще раньше, в 2012 г.

Невысокие показатели цитирования в 2019 г. для данных областей ИБ (как было выявлено, они наблюдаются и для других областей ИБ в этом году), объясняются, очевидно, известной причиной: замедленным «откликом» научного сообщества на публикации текущего года.

На рис. 3 и 4 представлена динамика востребованности итогов исследований российских ученых по обоим указанным направлениям.

Как следует из рис. 3, после четырехлетней стабильной востребованности итогов исследований в области управления ИБ, с 2015 г. наблюдается падение этого показателя более чем в 1,5 раза, вызванного, возможно, кризисом 2014 г. В области квантовой криптографии после максимума в 2011 г. востребованность резко (практически в три раза) упала с 2015 г. (рис. 4).

Максимальный индекс V среди всех вышеуказанных направлений исследований в сфере ИБ наблюдался в области кибербуллинга, минимальный – в сфере DLP-систем.

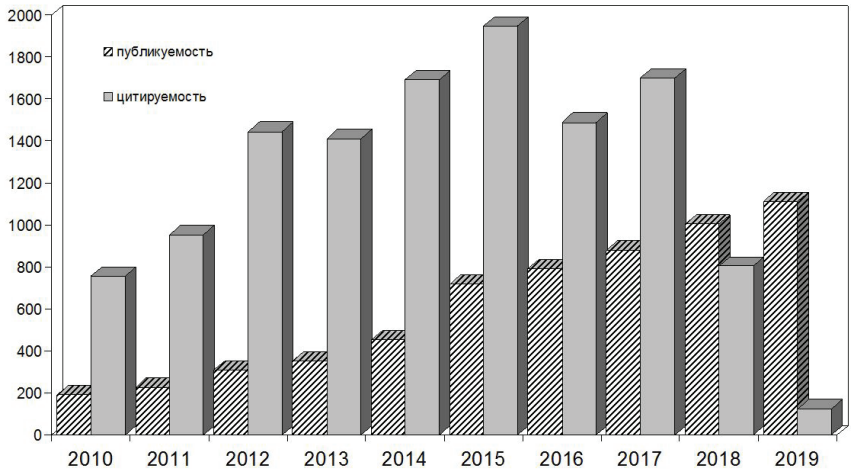

Рис. 1. Показатели публикационной активности и цитируемости российских ученых в 2010–2019 гг. в области управления информационной безопасностью

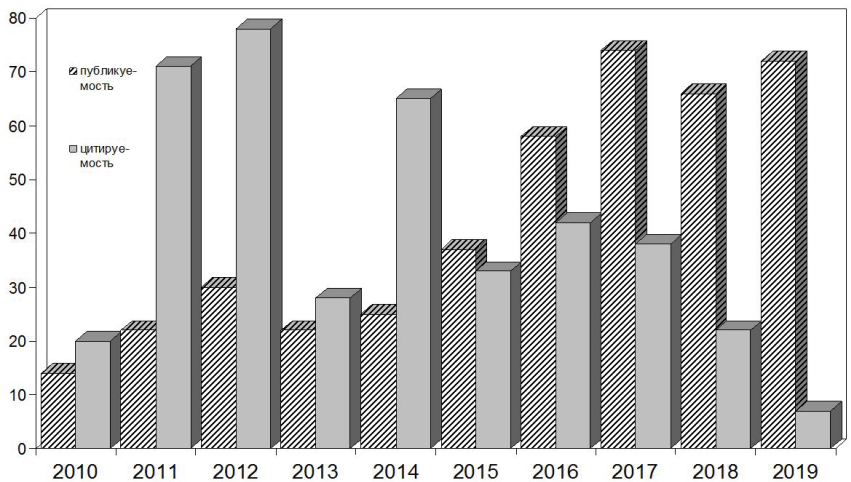

Рис. 2. Показатели публикационной активности и цитируемости российских ученых в 2010–2019 гг. в области квантовой криптографии

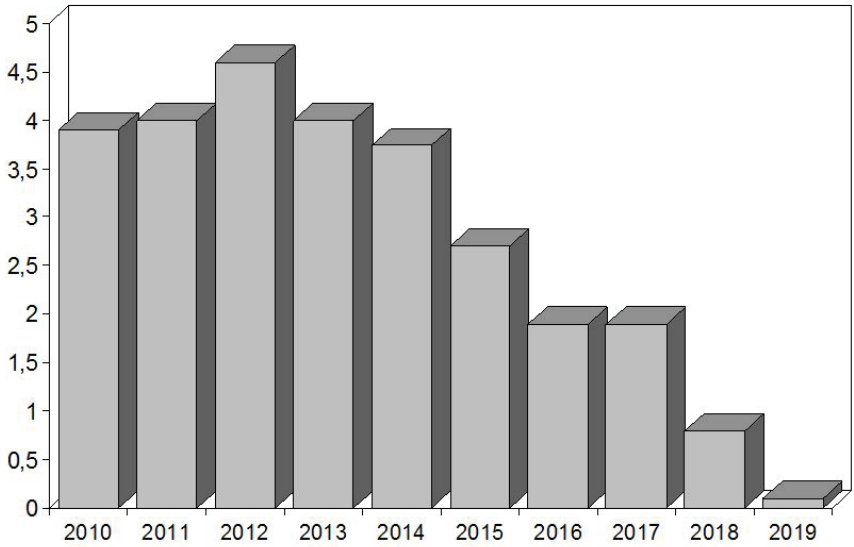

Рис. 3. Востребованность итогов исследований российских ученых в области управления информационной безопасностью

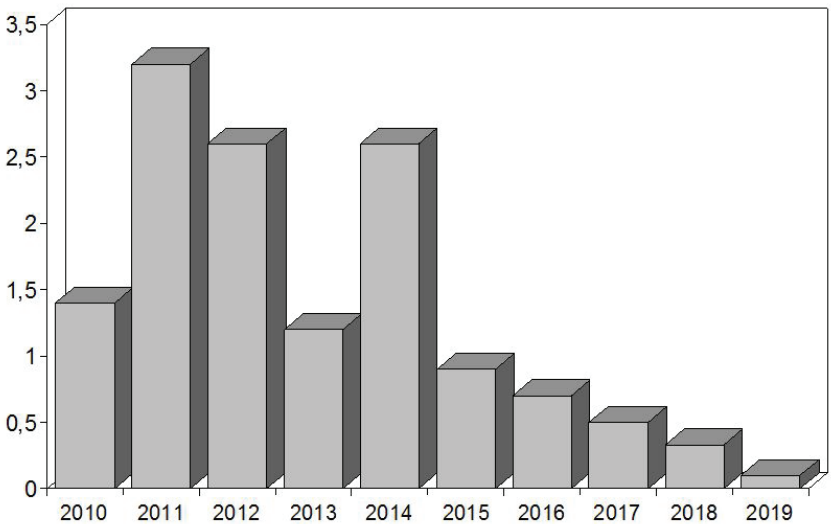

Рис. 4. Востребованность в 2010–2019 гг. итогов исследований российских ученых в области квантовой криптографии

Анализ максимумов публикационной активности для всех направлений в области ИБ показал, что практически все они сосредоточены в конце анализируемого периода. Так, для криптографии – это 2018 г.; максимумы в 2019 г. и 2017 г. для других направлений исследований в области ИБ представлены на рис. 5 и 6.

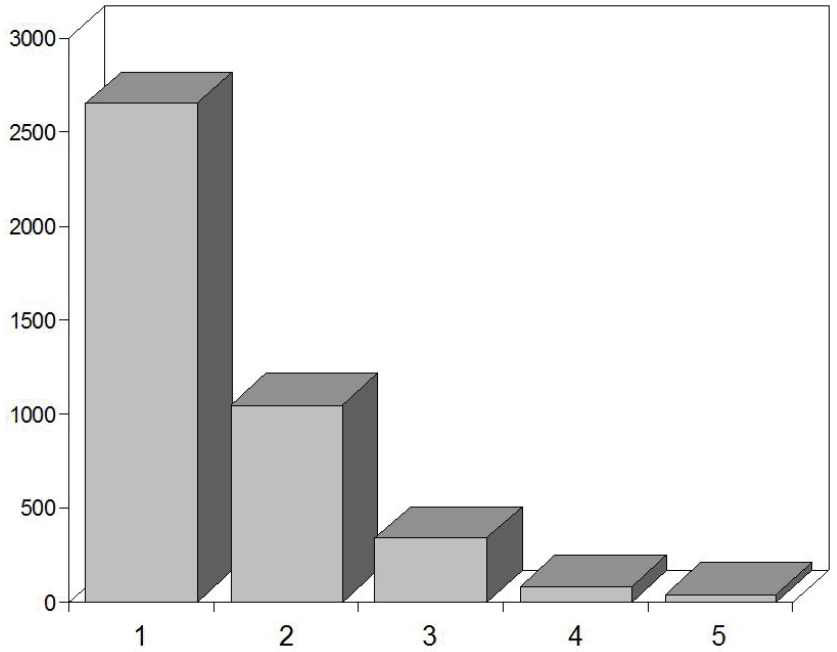

Рис. 5. Максимумы публикационной активности российских ученых в 2019 г., достигнутые в 2010–2019 гг. в направлениях исследований: 1 – технология блокчейн, 2 – управление ИБ, 3 – биометрические методы и средства защиты информации, 4 – квантовая криптография, 5 – методы обфускации

Из рисунков следует, во-первых, что для всех направлений ИБ отмечается рост числа публикаций вплоть до конца рассматриваемого периода, что объясняется все возрастающим интересом исследователей к итогам работ в этих областях, и, во-вторых, наибольшее значение публикационной активности отмечается в сфере технологии блокчейн, наименьшее – в области методов обфускации.

В отличие от публикационной активности максимумы цитируемости для различных направлений имеют свои особенности (рис. 7 и 8).

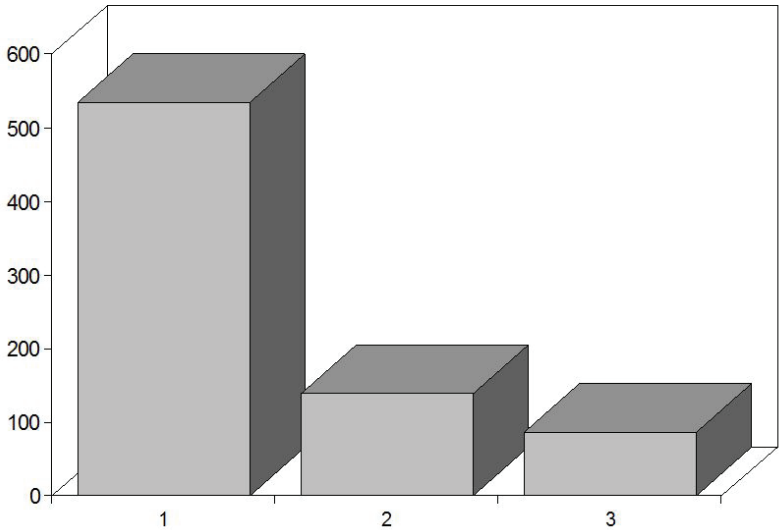

Рис. 6. Максимумы публикационной активности российских ученых в 2019 г., достигнутые в 2010–2019 гг. в направлениях исследований: 1– системы обнаружения вторжений, 2 – стеганография, 3 – DLP-системы

Максимумы цитируемости в области кибербуллинга и технологии блокчейн располагаются в конце исследуемого интервала; максимумы в сфере систем обнаружения вторжений и криптографии (включая квантовую криптографию) – в его начале, остальные (управление ИБ, биометрические методы и средства защиты информации, стеганография, DLP – системы, методы обфускации) – в середине интервала 2010–2019 гг. Из рис. 7 можно сделать вывод, что наибольший интерес научного сообщества практически в течение всего исследуемого периода вызывали результаты исследований в области технологии блокчейн и систем управления ИБ.

Наиболее высокие показатели востребованности (рис. 8) также наблюдались в сфере кибербуллинга и технологии блокчейн (они были достигнуты в середине исследуемого интервала); максимумы для остальных направлений исследований отмечались в первой половине интервала 2010–2019 гг.

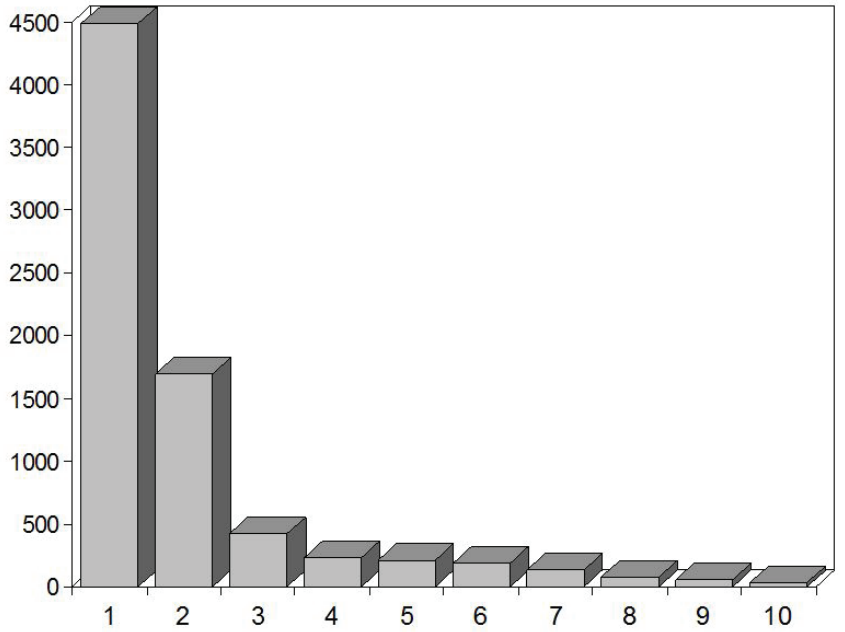

Рис. 7. Максимумы цитируемости российских ученых, достигнутые в 2010–2019 гг. в направлениях исследований: 1– технология блокчейн (2018), 2 – управление ИБ (2017), 3 – криптография (2012), 4 – системы обнаружения вторжений (2013), 5 – кибербуллинг (2019), 6 – биометрические методы и средства защиты информации (2016), 7 – стеганография (2016), 8 – квантовая криптография (2012), 9 – DLP-системы (2016), 10 – методы обфускации (2016) (в скобках указан год достижения максимума)

На рис. 9 представлены значения индекса Хирша H, характеризирующие множество публикаций P российских ученых и их цитируемость C в рассматриваемых областях исследований за 2010–2019 гг. Высокие показатели индекса Хирша, во-первых, свидетельствуют о том, что и в дальнейшем во всех анализируемых областях наук следует ожидать высоких значений P и C. Кроме того, как следует из рис. 9, выделяются три группы областей исследований: первая, в которую входят управление ИБ, технология блокчейн, криптография, биометрические методы и средства защиты и для которых индекс Хирша больше 15; вторая (кибербуллинг, системы обнаружения вторжений, стеганография), для которых H

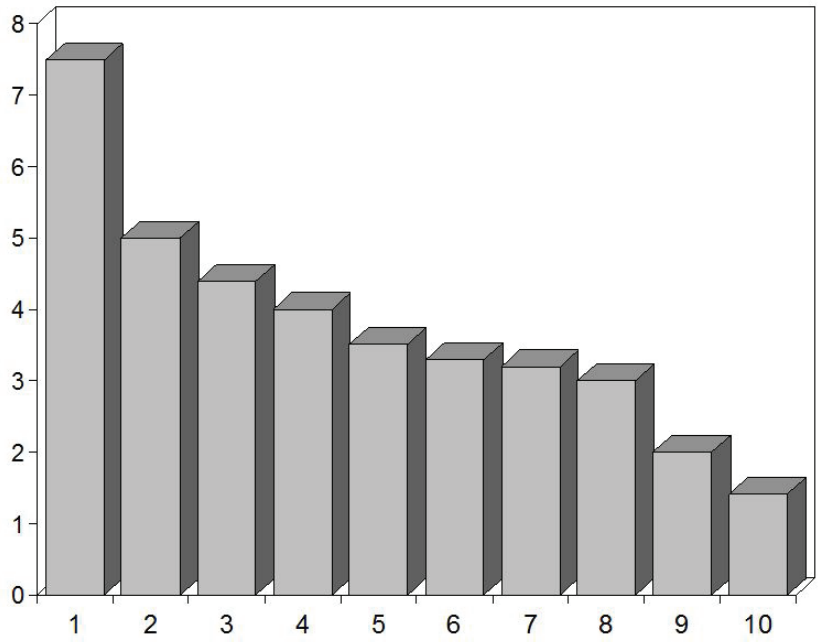

Рис. 8. Максимумы показателей востребованности итогов работ российских ученых, достигнутые в 2010–2019 гг. в следующих направлениях исследований: 1 – кибербуллинг, 2 – технология блокчейн, 3 – системы обнаружения вторжений, 4 – управление ИБ, 5 – биометрические методы и средства защиты, 6 – методы обфускации, 7 – квантовая криптография, 8 – криптография, 9 – стеганография, 10 – DLP- системы

равно 14, и третья (квантовая криптография, методы обфускации, DLP-системы), для которых индекс Хирша изменяется в интервале от 10 до 7.

В соответствии с классификацией, приводимой в работе [Ершова 2020], научная активность российских ученых первой группы соответствует мировому уровню научной активности, второй группы – национальному уровню, третьей группы – научной активности доктора наук.

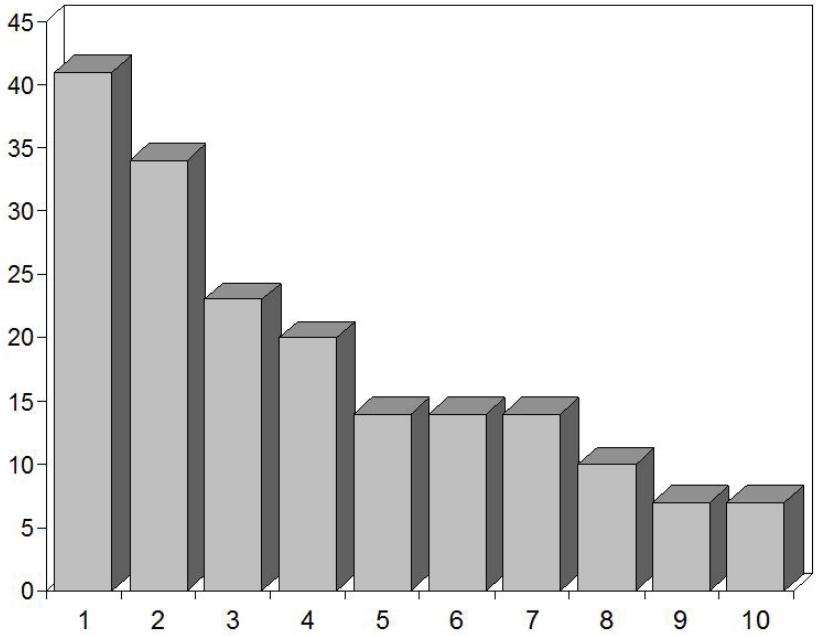

Рис. 9. Индексы Хирша, достигнутые российскими учеными за 2010–2019 гг. в направлениях исследований:
1 – управление ИБ, 2 – технология блокчейн, 3 – криптография, 4 – биометрические методы и средства защиты, 5 – кибербуллинг, 6 – системы обнаружения вторжений, 7 – стеганография, 8 – квантовая криптография, 9 – методы обфускации, 10 – DLP-системы
10 – DLP- системы

Заключение

По итогам выполненного исследования получены следующие основные результаты.

Впервые проанализирована динамика изменения наукометрических показателей научной деятельности (публикационной активности, цитируемости и индекса Хирша) в 2010–2019 гг. для актуальных направлений исследований в области ИБ, в число которых входят биометрические методы и средства защиты информации, технология блокчейн, криптография (включая квантовую криптографию), системы обнаружения вторжений.

(IDS-системы), стеганографические методы защиты информации, системы предотвращения утечки информации (DLP-системы), кибербуллинг, методы обфускации, управление информационной безопасностью. Анализ наукометрических показателей осуществлялся с использованием базы РИНЦ.

Выявлен ряд закономерностей этих показателей за анализируемый период, включая рост количества публикаций в течение всего исследуемого периода для следующих направлений исследований: технология блокчейн, управление ИБ, биометрические методы и средства защиты информации, квантовая криптография, методы обфускации. После четырехлетней стабильной востребованности итогов исследований в области управления ИБ с 2015 г. наблюдается падение этого показателя, вызванное, возможно, кризисом 2014 г.

Возрастание индекса цитирования до конца анализируемого периода отмечался лишь для двух направлений: технологии блокчейн и кибербуллинга. При этом максимум показателей востребованности итогов работ российских ученых, достигнутый российскими учеными, был выявлен в области кибербуллинга, минимум – в сфере DLP-систем.

Выявлены три группы областей исследований, отличающихся значениями индекс Хирша: первая, в которую входят управление ИБ, технология блокчейн, криптография, биометрические методы и средства защиты, для которых индекс Хирша больше 15; вторая (кибербуллинг, системы обнаружения вторжений, стеганография), для которых H равно 14, и третья (квантовая криптография, методы обфускации, DLP-системы), для которых индекс Хирша изменяется в интервале от 10 до 7. Отмечается, что научная активность российских ученых первой группы соответствует мировому уровню научной активности исследователей, второй группы – национальному уровню научной активности, третьей группы – научной активности доктора наук.

При этом выявленные высокие значения индекса Хирша для всех проанализированных направлений исследований в области ИБ свидетельствуют также о том, что и в дальнейшем в области информационной безопасности следует ожидать стабильную публикационную активность российских ученых по результатам их исследований.

Литература

Арутюнов 2009 – *Арутюнов В.В.* Типология и особенности современных коммуникаций в работе библиотек. М.: Литера, 2009 с.

Арутюнов 2013 – *Арутюнов В.В.* О результативности научной деятельности в области приоритетных направлений развития науки, технологий и техники // Научно-техническая информация. Сер. 1. № 10. С. 12–19.

Арутюнов 2015 – *Арутюнов В.В.* Особенности рейтинга цитируемости российских ученых по версии РИНЦ // Научные и технические библиотеки. 2015. № 5. С. 28–43.

Арутюнов 2020 – *Арутюнов В.В.* Наукометрические показатели исследователей-лидеров научной деятельности в области информационной безопасности // Вестник РГГУ, Серия «Информатика. Информационная безопасность. Математика». 2020. № 2. С. 46–56.

Арутюнов, Цветкова 2018 – *Арутюнов В.В., Цветкова В.А.* Сравнительный анализ показателей публикационной активности и цитируемости российских ученых в отдельных естественнонаучных областях знаний по данным РИНЦ и WOS CC // Информация и инновации. 2018. Т. 13. № 1. С. 22–27.

Донгак, Шатохин, Мещеряков 2019 – *Донгак Б.С., Шатохин А.С., Мещеряков Р.В.* Эффективность централизованного использования цифровых технологий, информационных ресурсов и средств защиты информации в органах власти на примере Республики Тыва // Известия Юго-Западного государственного университета. 2019. Т. 23. № 6. С. 99–114.

Ершова 2020 – *Ершова С.К.* Инструкция по использованию РИНЦ [Электронный ресурс] // Восточно-Европейский Институт психоанализа. URL: https://rf-gk.ru/profil-avtora-v-rinc-funkcionalnye-vozmozhnosti-rossiiskii/ (дата обращения 20 мая 2020).

Молчанова, Сканцев, Спасенников 2019 – *Молчанова Н.В., Сканцев В.М., Спасенников В.В.* Дискуссионные вопросы оценки эффективности научной деятельности с использованием индексов цитирования (обзор отечественных и зарубежных публикаций) // Эргодизайн. 2019. № 4 (6). С. 186–195.

РИНЦ 2020 – *РИНЦ:* Российский индекс научного цитирования [Электронный ресурс]. URL: https://elibrary.ru/querybox.asp?scope=newquery (дата обращения 20 марта 2020).

Ширяев, Доронина 2019 – *Ширяев А.А., Доронина Е.Г.* Методы повышения публикационной активности исследователей // Научно-техническая информация, сер. 1. 2019. № 11. С. 8–13.

Grinev 2019 – *Grinev A.V.* The use of scientometric indicators to evaluate publishing activity in modern Russia // Herald of the Russian Academy of Sciences. 2019. Т. 89. № 5. С. 451–459.

References

Arutyunov, V.V. (2009), *Typologiya i osobennosti sovremennykh kommunikatsiy v rabote bibliotek* [Typology and characteristics of modern communications in the work of libraries], Litera, Moscow, Russia.

Arutyunov, V.V. (2013), "On the scientific performance effectiveness in the field of priority areas for developing the science, technology and techniques", *Scientific and technical information,* ser. 1, vol. 10, pp. 12–19.

Arutyunov, V.V. (2015), "Features of the citation rating of Russian scientists according to the RSCI", *Scientific and technical libraries,* vol. 5, pp. 28–43.
Arutyunov, V.V. (2020), "Scientometric indicators for leaders in the scientific research of the information security", *RSUH/RGGU Bulletin. "Information Science. Information Security. Mathematics" Series*, vol. 2, pp. 46–56.
Arutyunov, V.V. and Tsvetkova, V.A. (2018), "Comparative analysis of indicators in the publication and citation of Russian scientists for certain natural science fields of knowledge according to the RSCI and WOS CC", *Information and innovations*, vol. 13, no. 1, pp. 22–27.
Dongak, B.S., Shatohin, A.S. and Mesheryakov, R.V. (2019), "The effectiveness of the centralized use of digital technologies, information resources, and data protection means in government bodies by the example of the Republic of Tyva", *News of South-western State University,* vol. 23, no. 6, pp. 99–104.
Grinev, A.V. (2019), "The use of scientometric indicators to evaluate publishing activity in modern Russia", *Herald of the Russian Academy of Sciences*, vol. 89, no. 5, pp. 451–459.
Ershova, S.K. (2020), "Instructions for using the RSCI", *East European Institute of Psychoanalysis* [Online], available at: https://rf-gk.ru/profil-avtora-v-rinc-funkcionalnye-vozmozhnosti-rossiiskii/ (Accessed 20 May 2020).
Molchanova, N.V, Skancev, V.M. and Spacennikov, V.V. (2019), "Discussion issues of assessing the effectiveness of scientific performance using citation indices (review of national and foreign publications)", *Ergodizain,* vol. 4 (6), pp. 186–195.
RSCI (2020), Russian Science Citation Index. [Online], https://elibrary.ru/querybox.asp?scope=newquery (Accessed 20 March 2020).
Shiryaev, A.A., and Doronina E.G. (2019), "Methods for increasing the publication activity researchers'", *Scientific and technical information,* ser. 1, vol.11, pp. 8–13.

Информация об авторе

Валерий В. Арутюнов, доктор технических наук, профессор, Российский государственный гуманитарный университет, Москва, Россия; 125993, Россия, Москва, Миусская пл., д. 6; warut698@yandex.ru

Information about the author

Valery V. Arutyunov, Dr. of Sci. (Computer Science), professor, Russian State University for the Humanities, Moscow, Russia; bld. 6, Miusskaya Sq., Moscow, Russia 125993; warut698@yandex.ru

УДК 004.3
DOI: 10.28995/2686-679X-2020-4-46-61

Разработка системы контроля целостности аппаратного оборудования в среде UEFI-BIOS

Александра А. Артамонова
Московский государственный технический университет им. Н.Э. Баумана, Москва, Россия, artamonova.a@yahoo.com

Андрей В. Куров
Московский государственный технический университет им. Н.Э. Баумана, Москва, Россия, avkur7@mail.ru

Аннотация. Разработка и производство компьютерных систем и компьютерного оборудования тесно связаны с вопросами обеспечения информационной безопасности и защиты данных. Одним из направлений в этой сфере является вопрос контроля целостности аппаратного оборудования для обнаружения и предотвращения добавления, удаления или замены устройств. Большинство существующих систем, решающих эту задачу, имеет ряд ограничений, среди которых может быть необходимость запуска под управлением операционной системы, наличие определенной версии BIOS или необходимость подключения специальных аппаратных компонентов. В статье предлагается метод, основная идея которого заключается в разработке UEFI-приложения, выполняющегося каждый раз при старте платформы до загрузки операционной системы, при первом запуске считывающего текущую конфигурацию устройств с помощью таблицы SMBIOS и низкоуровневых протоколов и сохраняющего ее в энергонезависимую память компьютера, а при последующих запусках сравнивающего текущую аппаратную конфигурацию с эталонной. В качестве аппаратной конфигурации для контроля предлагается использовать информацию об установленных процессорах, оперативной памяти, PCI-устройствах и жестких дисках. Такое приложение не будет зависеть от используемой версии BIOS, наличия операционной системы или определенной ее версии и не будет требовать наличия дополнительных аппаратных устройств.

Ключевые слова: UEFI, UEFI-приложение, SMBIOS, аппаратное обеспечение, контроль целостности

Для цитирования: Артамонова А.А., Куров А.В. Разработка системы контроля целостности аппаратного оборудования в среде UEFI-BIOS // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2020. № 4. С. 46–61. DOI: 10.28995/2686-679X-2020-4-46-61

Development of a hardware integrity monitoring system in the UEFI-BIOS environment

Aleksandra A. Artamonova
Bauman Moscow State Technical University, Moscow, Russia, artamonova.a@yahoo.com

Andrei V. Kurov
Bauman Moscow State Technical University, Moscow, Russia, avkur7@mail.ru

Abstract. The development and production of the computer systems and computer equipment are closely related to the issues of information security and data protection. One of the directions in that area is the issue of monitoring the hardware integrity to detect and prevent the addition, removal or replacement of devices. Most existing systems that solve the problem have a number of limitations, including the need to run under an operating system, the presence of a specific BIOS version, or the need to connect special hardware components. The article proposes a method, the main idea of which is to develop a UEFI application that runs every time the computer starts before loading the operating system. While the first start it performs reading of current device configuration using the SMBIOS table and low-level protocols and stores it in the non-volatile memory of the computer. On subsequent runs it compares the current hardware configuration with the saved one and detects differences. As a hardware configuration for integrity monitoring it is suggested to use information about installed CPUs, RAM devices, PCI devices and hard drives. Such an application does not depend on the BIOS version used, the operating system or a specific version of it, and does not require additional hardware devices.

Keywords: UEFI, UEFI-Application, SMBIOS, hardware, hardware integrity

For citation: Artamonova, A.A. and Kurov, A.V. (2020), "Development of a hardware integrity monitoring system in the UEFI-BIOS environment", *RSUH/RGGU Bulletin. "Information Science. Information Security. Mathematics" Series*, no. 4, pp. 46–61, DOI: 10.28995/2686-679X-2020-4-46-61

Введение

Разработка и производство компьютерных систем и компьютерного оборудования тесно связаны с вопросами обеспечения информационной безопасности и защиты данных. Решение этих задач обычно является комплексным и может включать в себя рассмотрение целого ряда проблем, среди которых присутствуют защита конфиденциальной информации от несанкционированного доступа, защита от мошеннических атак, защита интеллектуальной собственности от пиратства и т. д. Одним из направлений решения поставленной задачи является контроль состава аппаратного оборудования, который можно рассматривать по-разному в зависимости от требуемой сферы применения и необходимой степени защиты.

Сфера информационной безопасности успешно развивается, и по мере ее эволюции предлагаются различные подходы для надежного решения поставленных задач. Однако существует целый ряд ситуаций, в которых высокий уровень защиты не является обязательным, но может быть достигнут зачастую только использованием сложного и/или дорогостоящего решения. В качестве примера, когда необходим контроль аппаратного оборудования но использования сложной системы защиты не требуется, можно привести производство компьютерных систем с предоставлением гарантийного обслуживания. Заказчик оборудования при нарушении порядка использования оборудования и неудачной попытке обхода установленных производителем средств защиты интеллектуальной собственности должен нести ответственность в правовом поле, поэтому ясно, что использование дорогостоящих высокотехнологичных средств защиты информации в подобной ситуации является избыточным, а более простое решение, пусть и не такое надежное, оказывается более предпочтительным. Другим примером является обнаружение и предотвращение попыток хищения аппаратных компонент на рабочем месте сотрудниками компаний: вероятная выгода, которую злоумышленник сможет извлечь с учетом всех рисков, вряд ли будет выше, чем затраты на обход установленных средств защиты, даже если они не будут отвечать высоким стандартам безопасности.

В качестве минимального требования к системе безопасности, обладающей указанными особенностями, можно выделить наличие возможности определения целостности аппаратных компонент с целью обнаружения их добавления или изъятия. В этом случае существующие решения, удовлетворяющие поставленному требованию, можно условно разделить на три группы: программные высокого уровня, программные низкого уровня и программно-аппаратные (с программной логикой низкого уровня).

Решения, принадлежащие к первой категории (например, Secret Net Studio[1]), отличаются тем, что доступ к их функциям может осуществляться только из операционной системы. К явным преимуществам таких систем можно отнести то, что разработка собственной системы этого уровня при необходимости не будет представлять особой сложности (если использование существующих решений по каким-либо причинам будет неприемлемо). Однако данный подход накладывает ряд ограничений, в частности, необходимость использования конкретной операционной системы (и в принципе использование любой операционной системы), из-за чего такие решения не отличаются универсальностью. Кроме того, это означает, что администратор или компания-производитель должны отвечать за установку этой операционной системы и последующую конфигурацию программных средств защиты.

Другой подход, включающий в себя использование низкоуровневых программных систем защиты, решает проблему зависимости от наличия операционной системы. К таким системам можно отнести многие из версий BIOS, в которые уже встроен подобный функционал (например, AMI BIOS[2]). В таких версиях BIOS можно настроить вывод предупреждений о замене аппаратных компонент и даже блокировку загрузки операционной системы в данном случае, а некоторые из них поддерживают также датчики вскрытия корпуса компьютера. К недостаткам данного подхода можно отнести зависимость от конкретной версии BIOS, и, следовательно, зависимость от производителя материнской платы, а также отсутствие гибкости настройки поведения в случае обнаружения несанкционированного доступа. Существуют и другие решения (например, ViPNet SafeBoot[3]), независимые от BIOS, однако они являются коммерческими, и алгоритмы их работы нельзя найти в открытом доступе.

Аппаратно-программные средства защиты (например, средство доверенной загрузки Dallas Lock[4]) не зависят ни от операционной системы, ни от платформы, ни от версии BIOS. Такие системы включают в себя аппаратную часть (как правило, плату расшире-

---

[1] Secret Net Studio [Электронный ресурс]. URL: https://www.securitycode.ru/products/secret-net-studio (дата обращения 10 декабря 2020).

[2] BIOS/UEFI Firmware [Электронный ресурс]. URL: https://ami.com/en/products (дата обращения 10 декабря 2020).

[3] ViPNet SafeBoot [Электронный ресурс]. URL: https://infotecs.ru/product/vipnet-safeboot.html (дата обращения 10 декабря 2020).

[4] СДЗ Dallas Lock [Электронный ресурс]. URL: https://dallaslock.ru/products/sdz-dallas-lock (дата обращения 10 декабря 2020).

ния с собственной энергонезависимой памятью) и программную, которая реализует функционал, контролирующий текущее состояние аппаратной конфигурации системы. К очевидным недостаткам таких систем можно отнести необходимость подключения дополнительных аппаратных компонентов, что может привести к невозможности использования таких систем на некоторых платформах (например, на ноутбуках).

В данной статье предлагается низкоуровневое программное решение для контроля целостности аппаратных компонент, которое не зависит от наличия операционной системы, конкретной версии BIOS и не требует подключения дополнительных аппаратных компонент. Основная идея предлагаемого метода заключается в разработке UEFI-приложения, которое встраивается в микросхему BIOS и хранит свои настройки в энергонезависимой памяти компьютера. При первом запуске компьютера UEFI-приложение считывает с помощью таблиц SMBIOS и низкоуровневых протоколов текущую аппаратную конфигурацию системы и сохраняет ее в качестве эталонной, а при последующих – сравнивает текущую конфигурацию с сохраненной и в случае обнаружения несоответствий выводит предупреждение. В качестве аппаратной конфигурации для сравнения предлагается использовать информацию об установленных процессорах, оперативной памяти, PCI-устройствах и жестких дисках.

Программная реализация системы

- UEFI-образ – это формат исполняемого содержимого, с помощью которого развертывается программный код. Все UEFI-образы содержат заголовок PE/COFF (Portable Executable Common Object File Format), который определяет формат исполняемого кода в соответствии со спецификацией [Microsoft 2020]. Целевым объектом этого кода может быть процессор IA-32, процессор Itanium®, x64, ARM или процессор с поддержкой EFI Byte Code (EBC). Заголовок определяет тип процессора и тип образа. В настоящий момент существует три типа UEFI-образов [Zimmer, Rothman, Marisetty 2010]:
- UEFI-приложения (англ. UEFI applications) – образы, память и состояние которых очищаются (сбрасываются) при завершении;
- UEFI-драйверы периода загрузки (англ. UEFI Boot Service drivers) – образы, память и состояние которых сохраняются на протяжении всего времени работы предварительной загрузки операционной системы. Их память очищается

при вызове загрузчиком операционной системы функции ExitBootServices();

- UEFI-драйверы периода выполнения (англ. UEFI Runtime drivers) – образы, память и состояние которых сохраняются на протяжении всего времени работы машины. Эти образы работают совместно с операционной системой, поддерживающей UEFI.

Кроме того, доступно несколько поддерживаемых мест хранения UEFI-образов, в их числе:

- ПЗУ (ROM) на PCI-карте;
- системное ПЗУ или системная флеш-память;
- мультимедийное устройство (например, жесткий диск, дискета, DVD);
- загрузочный LAN-сервер.

Поскольку система проверки целостности аппаратной конфигурации должна запускаться непосредственно на целевом устройстве без использования каких-либо накопителей и не должна предоставлять доступ к своим данным для других UEFI-образов, в качестве типа образа используется UEFI-приложение, а в качестве расположения – Flash ROM-память, в которой находится образ BIOS. В качестве места для хранения своих настроек система использует NVRAM-память, энергонезависимую память компьютера.

Программный код UEFI-BIOS состоит из различных пакетов, которые, в свою очередь, являются логическим объединением определенного количества модулей – наименьших фрагментов отдельно компилируемого или предварительно созданного кода [Tianocore 2018b]. Каждый пакет имеет одинаковую структуру каталогов для разделения файлов исходного кода. Каждый пакет может включать в себя следующие корневые каталоги: *Include*, *Library*, *Application*, *Drivers*. Каталог *Include* содержит заголовочные файлы, предназначенные для использования другими пакетами. В каталоге *Library* находятся подкаталоги для каждого модуля библиотеки в составе пакета. Аналогичным образом каталог *Application* включает в себя подкаталоги для каждого модуля приложения, а *Driver* – подкаталоги для модулей драйверов. При использовании системы сборки EDKII в каталоге пакета также должны находиться DEC-файл декларации пакета и DSC-файл с инструкциями для сборки, а в подкаталоге каждого из модулей – INF-файл метаданных.

Структура пакета, реализующего систему проверки целостности аппаратной конфигурации, представлена на рис. 1.

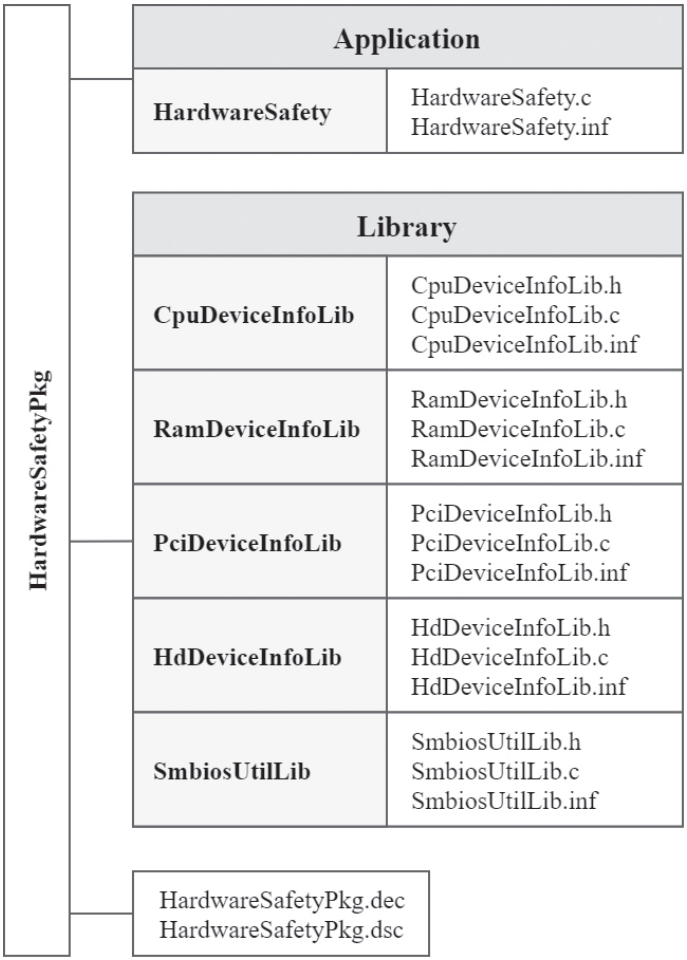

Рис. 1. Структура пакета HardwareSafetyPkg

Файл исходного кода *HardwareSafety.c* содержит основную точку входа в приложение, реализацию функций пользовательского интерфейса и функций для работы с NVRAM-памятью для чтения и записи конфигурации устройств, а также вызовы необходимых функций из библиотек устройств.

Библиотеки устройств отвечают за реализацию функционала для работы с каждым из четырех типов поддерживаемых аппаратных компонентов – процессоры (*CpuDeviceInfoLib*), оперативная память (*RamDeviceInfoLib*), PCI-устройства (*PciDeviceInfoLib*)

и жесткие диски (*HdDeviceInfoLib*). Кроме того, для получения информации о процессорах и установленной оперативной памяти используется вспомогательная библиотека для удобной работы с таблицей SMBIOS (*SmbiosUtilsLib*). DSC-файл содержит информацию для систем сборки, а в DEC-файле и INF-файлах находится конфигурационная информация о пакете и модулях соответственно.

Способ получения информации об аппаратных компонентах отличается в зависимости от их типа, однако для удобства использования все библиотеки устройств построены по единому принципу. В заголовочных файлах (*CpuDeviceInfoLib.h*, *RamDeviceInfoLib.h*, *PciDeviceInfoLib.h* и *HdDeviceInfoLib.h)* находятся описания идентификационной информации об устройстве конкретного типа и общей конфигурации этих устройств, которая включает в себя их количество и массив с указателями на соответствующие структуры с информацией для идентификации. Кроме того, здесь располагаются прототипы двух функций, доступных вне библиотеки: получение текущего состояния конфигурации этих аппаратных компонентов и сравнение двух конфигураций данного типа. Реализации этих функций находятся, соответственно, в соответствующих файлах исходного кода (*CpuDeviceInfoLib.c*, *RamDeviceInfoLib.c*, *PciDeviceInfoLib.c* и *HdDeviceInfoLib.c*).

Каждый тип устройств обладает своей спецификой получения данных о конфигурации. Для доступа к информации об установленных процессорах и оперативной памяти используется таблица SMBIOS. Таблица SMBIOS состоит из точки входа и переменного числа структур, описывающих компоненты и функции платформы, которые обычно называют таблицами или записями [DMTF 2020]. Информация в таблице обновляется каждый раз при запуске системы до запуска UEFI-образов [Unified Extensible Firmware 2019], что гарантирует актуальность считанной конфигурации устройств на стадии запуска UEFI-приложения. Реализации вспомогательных функций для чтения записей этой таблицы находятся в файле исходного кода *SmbiosInfo.c*.

Для каждого из процессоров в SMBIOS определена таблица типа EFI_SMBIOS_TYPE_PROCESSOR_INFORMATION, которая содержит специфичную для него информацию (тип, версия, производитель, серийный номер и т.д.). Для каждого из устройств оперативной памяти существует аналогичная таблица EFI_SMBIOS_TYPE_MEMORY_DEVICE. По причине того, что эта информация заполняется производителем и набор информационных полей может отличаться в зависимости от модели устройства, значения некоторых полей могут отсутствовать. Сравнение не одного поля (например, только серийного номера), а всей инфор-

мации в совокупности делает проверку изменения конфигурации более надежной.

Список полей, составляющих идентификационную информацию для процессоров (структура CpuDevice) и оперативной памяти (структура RamDevice) вместе с примерами заполненного содержимого приведен в табл. 1 и табл. 2 соответственно. После получения информации об установленных устройствах остается только подсчитать их количество и сохранить необходимые данные в переменную конфигурации.

Таблица 1

Поля структуры,
описывающей устройство типа CpuDevice

Название поля	Пример содержимого
ProcessorType	Central Processor
ProcessorFamily	Intel(R) Core(TM) i5
ProcessorManufacturer	Intel(R) Corporation
ProcessorId	EA 06 09 00 FF FB EB BF
ProcessorVersion	Intel(R) Core(TM) i5-8400 CPU @ 2.80GHz
MaxSpeed	8300
SerialNumber	MC515299A1605

Таблица 2

Поля структуры,
описывающей устройство типа RamDevice

Название поля	Пример содержимого
Size	8192
FormFactor	DIMM
DeviceLocator	ChannelB-DIMM0
Speed	0x855
Manufacturer	Foxline
SerialNumber	23C951AC
PartNumber	FL2133D4U15-8G

В связи с тем что таблица SMBIOS предоставляет недостаточно информации для идентификации PCI-устройств и не содержит никаких данных об установленных жестких дисках, для получения этих конфигураций приложение использует внутренние протоколы UDKII[5], EFI_PCI_ROOT_BRIDGE_PROTOCOL и EFI_DISK_INFO_PROTOCOL соответственно. Во время инициализации UEFI происходит заполнение базы данных дескрипторов (англ. handle database), состоящей из дескрипторов и протоколов, с помощью которых регистрируются все вызываемые интерфейсы [Zimmer, Rothman, Marisetty 2010]; таким образом можно получить доступ к информации о соответствующих аппаратных компонентах. Интерфейсы, предоставляемые этими протоколами, скрывают специфические для платформы детали реализации и упрощают доступ к устройствам [Tianocore 2018a].

Информация об устройствах PCI и PCI-Express располагается в регистрах конфигурационного пространства PCI, доступ к которым осуществляется путем отправки команд конфигурации контроллеру PCI. Для этого сначала необходимо получить массив дескрипторов, поддерживающих протокол EFI_PCI_ROOT_BRIDGE_PROTOCOL, при помощи функции gBS->LocateHandleBuffer(). Каждое из PCI-устройств обладает уникальным топологическим адресом, состоящим из номера шины (англ. Bus) и номеров физического (англ. Device) и логического (англ. Function) устройств [Budruk, Anderson, Shanley 2003]. Прямого метода определения слотов с установленными PCI-устройствами из среды UEFI-BIOS нет, поэтому необходимо просканировать все возможные адреса, изменяя значения номеров шин и устройств в возможных диапазонах (Bus от 0 до 255, Device от 0 до 31, Function от 0 до 7) и для каждого из вариантов осуществить попытку чтения нулевого регистра, в котором содержится информация об идентификаторе устройства (англ. Device ID, DID) и идентификаторе производителя (англ. Vendor ID, VID). Для этого требуется вычислить значение базового адреса, который состоит из номера шины, номера физического устройства и номера логического устройства при нулевом значении регистра, основываясь на формате конфигурационного адреса [PCI specification] и выполнив необходимые преобразования типов:

```
(UINT64) (((UINTN) Bus << 24) + ((UINTN) Dev << 16) + ((UINTN) Func << 8)).
```

[5] UDK2018 [Электронный ресурс]. URL: https://github.com/tianocore/tianocore.github.io/wiki/UDK2018 (дата обращения 10 декабря 2020).

Теперь можно получить информацию об устройстве при помощи функции Pci->Read(), передав ей в качестве параметра вычисленное значение адреса, и в случае успешной попытки чтения она вернет необходимую информацию об обнаруженном устройстве. Список полей, составляющих идентификационную информацию для PCI-устройств (структура PciDevice) с примерами заполненного содержимого, приведен в табл. 3. Значение идентификатора производителя выдается организацией PCI SIG, а значение идентификатора устройства назначается его производителем; при этом каждое из полей, указанных в табл. 3, является обязательным для любого PCI-устройства [Budruk, Anderson, Shanley 2003].

Таблица 3

Поля структуры,
описывающей устройство типа SataDevice

Название поля	Пример содержимого
VendorId	8086
DeviceId	27D0
ClassCode	0604
RevisionId	02

Для получения доступа к информации о жестких дисках необходимо, как и в случае с PCI-устройствами, сначала получить массив дескрипторов, поддерживающих протокол EFI_DISK_INFO_PROTOCOL_GUID. Для каждого элемента массива следует выполнить обращение к функции gBS->HandleProtocol(), чтобы определить, поддерживает ли выбранный дескриптор данный протокол. В случае успеха для полученного экземпляра устройства необходимо вызвать команду Identify(), предварительно назначив интерфейс (IDE или AHCI): в случае, если конкретное устройство не поддерживает взаимодействие в выбранном режиме (например, если это USB-устройство), происходит переход к следующему дескриптору. Список полей, составляющих идентификационную информацию для жестких дисков (структура HdDevice) с примерами заполненного содержимого приведен, в табл. 4.

Как видно из таблиц 1-4, списки полей, в совокупности составляющих идентификационную информацию для каждого типа устройств, могут с приемлемой точностью гарантировать ее уникальность для каждого из аппаратных компонент, особенно при возможности первоначальной настройки, включающей в себя заполнение необходимых полей данных в таблице SMBIOS.

Таблица 4

Поля структуры,
описывающей устройство типа HdDevice

Название поля	Пример содержимого
ModelName	INTEL SSDSC2BW480A4
SerialNo	CVDA505400524605GN

UEFI-приложение обладает текстовым пользовательским интерфейсом для просмотра текущей аппаратной конфигурации, сохранения новой или для отключения ее проверки, однако доступ к этим возможностям есть только в меню управления, войти в которое возможно при наличии у пользователя прав администратора. Для лаконичности вывода в меню управления аппаратной конфигурацией отображается не вся хранимая информация об устройствах, а только ее часть, хотя при сравнении идет проверка всех полей. Пароль хранится в энергонезависимой памяти компьютера NVRAM в хешированном виде с использованием алгоритма SHA256; администратор может изменить его в меню управления.

В текущей реализации средства защиты не блокируют дальнейшую загрузку операционной системы в случае обнаружения нарушения целостности аппаратной конфигурации, а только выводят сообщение об этом, однако данная функция может быть добавлена в дальнейшем при их модернизации. Для того чтобы у пользователей устройства была возможность ознакомиться с предупреждениями о нарушении целостности при их возникновении и ввести пароль администратора, UEFI-приложение после своего запуска выводит текстовое меню с пунктами пользовательского интерфейса. После этого начинается обратный отсчет времени таймаута, равного десяти секундам, после окончания которого приложение завершает свою работу и возобновляется обычная загрузка операционной системы. Если пользователь нажмет любую клавишу, кроме клавиши входа в главное меню, работа приложения также будет завершена. В случае, если будет обнаружено нарушение целостности аппаратной конфигурации (например, при удалении одного из устройств), а затем она будет восстановлена (при подключении того же устройства), предупреждения не исчезнут, но появится пояснение о том, что хотя целостность оборудования была нарушена ранее, в настоящий момент конфигурация соответствует эталонной. При отключении проверки или сохранении новой эталонной аппаратной конфигурации все предупреждения сбрасываются. По умолчанию контроль целостности отключен.

Пример работы приложения приведен на рис. 2 и 3. При первом запуске компьютера после встраивания образа UEFI-приложения в образ BIOS аппаратная конфигурация компьютера была сохранена в качестве эталонной (рис. 2). Затем установленный жесткий диск был удален, а вместо него подключен другой диск. При следующем запуске приложения было выведено предупреждение о нарушенной целостности аппаратной конфигурации с указанием того, какое устройство было добавлено, а какое – удалено (рис. 3).

```
================================================================================================
Текущая конфигурация:
Устройства PCI
VID: 8086 PID: 3EC2
VID: 8086 PID: 3E92
VID: 8086 PID: A2AF
VID: 8086 PID: A2B1
VID: 8086 PID: A2BA
VID: 8086 PID: A294
VID: 8086 PID: A2CA
VID: 8086 PID: A2A1
VID: 8086 PID: A2F0

Процессор
Intel(R) Core(TM) i5-8400 CPU @ 2.80GHz

Оперативная память
Manufacturer: Foxline  Model: FL2133D4U15-8G  S\N: 23C951AC  Size: 8192 MB  Speed: 2133 Hz

Жесткие диски
Model Name: HGST HTS545050A7E680  S\N: RB250A263TZ9GJ

Контроль целостности аппаратной конфигурации включен

Нажмите 'E' для сохранения новой эталонной конфигурации
Нажмите 'N' для выключения инвентаризации
================================================================================================
Нажмите 'Q' для возврата в главное меню
```

Рис. 2. Вывод текущей аппаратной конфигурации компьютера из меню управления

```
Внимание! Нарушена целостность аппаратной конфигурации
Жесткий диск был удален. Model Name: HGST HTS545050A7E680  S\N: RB250A263TZ9GJ
Жесткий диск был добавлен. Model Name: INTEL SSDSC2BW480A4  S\N: CVDA505400524605GN

Нажмите 'C' для входа в режим управления
. . .
Введите пароль для входа в режим управления: ********
```

Рис. 3. Вывод предупреждения при нарушенной целостности аппаратной конфигурации компьютера

Это предупреждение будет выводиться при каждом запуске компьютера (и, соответственно, приложения) до тех пор, пока администратор не сохранит новую эталонную конфигурацию или не отключит проверку в меню управления, войти в которое он может, нажав клавишу ‘C’ без ожидания окончания отсчета таймаута после запуска приложения.

Заключение

В статье предлагается метод проверки целостности аппаратной конфигурации, основанный на использовании низкоуровневого приложения, работающего в среде UEFI-BIOS. Работа системы не зависит от наличия операционной системы и от используемой версии BIOS, а также не требует для своего функционирования подключения дополнительных аппаратных компонентов. Приложение начинает свое выполнение после прохождения основных фаз загрузки базовой системы ввода-вывода, осуществляет проверку целостности аппаратной конфигурации, выводит предупреждение в случае нарушения целостности. Если пользователь не нажмет клавишу для входа в меню управления, по истечении временного интервала, отсчитываемого таймером, оно завершает свою работу, передавая управление загрузчику операционной системы. Однако такая система может быть полезной, только если контролирующая сторона (производитель оборудования или администратор) будет иметь доступ к устройству (например, при проверке выполнения условий эксплуатации для определения возможности гарантийного обслуживания). В качестве дальнейших направлений усовершенствования системы можно перечислить следующие: выполнение шифрования сохраненной эталонной конфигурации для предотвращения ее изменения в NVRAM-памяти; определение факта вскрытия корпуса при наличии встроенного датчика на материнской плате; добавление возможности блокировки загрузки операционной системы при обнаружении вскрытия.

Литература

Budruk, Anderson, Shanley 2003 – *Budruk R., Anderson D., Shanley T.* PCI Express System Architecture. Boston, MA: Addison-Wesley Developer’s Press, 2003.

DMTF 2020 – DMTF. System Management BIOS (SMBIOS) Reference Specification Version 3.4.0 [Электронный ресурс]. URL: https://www.dmtf.org/sites/default/files/standards/documents/DSP0134_3.4.0.pdf (дата обращения 10 декабря 2020).

Microsoft 2020 – Microsoft, PE Format [Электронный ресурс]. URL: https://docs.microsoft.com/en-us/windows/win32/debug/pe-format (дата обращения 10 декабря 2020).

Tianocore 2018a – Tianocore, EDK II Driver Writer's Guide [Электронный ресурс]. URL: https://edk2-docs.gitbook.io/edk-ii-uefi-driver-writer-s-guide (дата обращения 10 декабря 2020).

Tianocore 2018b – Tianocore, EDK II Module Writer's Guide [Электронный ресурс]. URL: https://edk2-docs.gitbook.io/edk-ii-module-writer-s-guide (дата обращения 10 декабря 2020).

Unified Extensible Firmware 2019 – Unified Extensible Firmware Interface (UEFI) Specification Version 2.8 [Электронный ресурс]. URL: https://uefi.org/sites/default/files/resources/UEFI_Spec_2_8_final.pdf (дата обращения 10 декабря 2020).

Zimmer, Rothman, Marisetty 2010 – *Zimmer V., Rothman M., Marisetty S.* Beyond BIOS: Developing with the Unified Extensible Firmware Interface, 2nd ed. Hudson, MA: Intel Press, 2010.

References

Budruk R., Anderson D. and Shanley T. (2003), *PCI Express System Architecture,* Addison-Wesley Developer's Press, Boston, USA.

DMTF, System Management BIOS (SMBIOS) Reference Specification Version 3.4.0 (2020), [Online], available at: https://www.dmtf.org/sites/default/files/standards/documents/DSP0134_3.4.0.pdf (Accessed 10 December 2020).

Microsoft, PE Format (2020), [Online], available at: https://docs.microsoft.com/en-us/windows/win32/debug/pe-format (Accessed 10 December 2020).

Tianocore, EDK II Driver Writer's Guide (2018), [Online], available at: https://edk2-docs.gitbook.io/edk-ii-uefi-driver-writer-s-guide (Accessed 10 December 2020).

Tianocore, EDK II Module Writer's Guide (2018), [Online], available at: https://edk2-docs.gitbook.io/edk-ii-module-writer-s-guide (Accessed 10 December 2020).

Unified Extensible Firmware Interface (UEFI) Specification Version 2.8 (2019), [Online], available at: https://uefi.org/sites/default/files/resources/UEFI_Spec_2_8_final.pdf (Accessed 10 December 2020).

Zimmer V., Rothman M. and Marisetty S. (2010), *Beyond BIOS: Developing with the Unified Extensible Firmware Interface*, 2nd ed., Intel Press, Hudson, USA.

Информация об авторах

Александра А. Артамонова, студент, Московский государственный технический университет имени Н.Э. Баумана, Москва, Россия; 105005, Россия, Москва, 2-я Бауманская ул., д. 5; artamonova.a@yahoo.com

Андрей В. Куров, кандидат технических наук, доцент, Московский государственный технический университет имени Н.Э. Баумана, Москва, Россия; 105005, Россия, Москва, 2-я Бауманская ул., д. 5; avkur7@mail.ru

Information about the authors

Aleksandra A. Artamonova, student, Bauman Moscow State Technical University, Moscow, Russia; bld. 5, 2nd Bauman Str., Moscow, 105005, Russia; artamonova.a@yahoo.com

Andrey V. Kurov, Cand. of Sci. (Computer Engineering), associate professor, Bauman Moscow State Technical University, Moscow, Russia; bld. 5, 2nd Bauman Str., Moscow, 105005, Russia; avkur7@mail.ru

УДК 519.81:069
DOI: 10.28995/2686-679X-2020-4-62-71

Применимость метода ELECTRE I для оценки многокритериальных альтернатив в задачах выбора принципа управления доступом к музейным цифровым копиям

Максим В. Шептунов

Российский государственный гуманитарный университет, Москва, Россия;
Московский государственный лингвистический университет, Москва, Россия, triumf403@yandex.ru

Аннотация. Выяснена применимость метода ELECTRE I – одного из методов разработки индексов попарного сравнения альтернатив – для поддержки решений при управлении информационными ресурсами в ракурсе выбора принципа предоставления доступа к ним с учетом различных информационных рисков. Показана перспективность данного многокритериального метода поддержки решений для анализа и снижения этих рисков, трудных для их учета другими методами принятия и поддержки решений даже в случае лишь трех критериев выбора при их противоречивости, имеющих место при цифровизации музейной сферы. В статье метод ELECTRE I рассматривается как способ обоснования выбора защитных мер в ракурсе одного из принципов разграничения доступа в отношении оцифрованных и вновь производимых копий музейных экспонатов.

В качестве возможного иллюстративного примера применения взяты три представляющихся весьма существенными для музейно-выставочного дела критерия при выборе одного из 2-х наиболее известных принципов управления доступом как к уже созданным, так и к еще создаваемым при разграничиваемом доступе цифровым копиям: 1) среднее время проникновения злоумышленника в автоматизированную систему защищенной обработки информации; 2) время на создание и разборку музейной экспозиции с учетом процессов аутентификации и авторизации; 3) стоимость создания либо модернизации подсистемы защиты информации.

Ключевые слова: информационные риски, альтернативы, многокритериальное принятие решений, цифровые музейные копии, защитные меры

Для цитирования: Шептунов М.В. Применимость метода ELECTRE I для оценки многокритериальных альтернатив в задачах выбора принципа управления доступом к музейным цифровым копиям // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2020. № 4. С. 62–71. DOI: 10.28995/2686-679X-2020-4-62-71

Applicability of the ELECTRE I method for multi-evaluating alternatives in tasks for selecting the access control principle to the museum digital copies

Maksim V. Sheptunov

Russian State University for the Humanities, Moscow, Russia;
Moscow State Linguistic University, Moscow, Russia,
triumf403@yandex.ru

Abstract. The article considers an applicability of the ELECTRE I method, scilicet one of the methods for developing indices of pairwise comparison in alternatives, for the decision support when managing the information resources in terms of choosing the principle providing an access to them, with due account for various information risk. It proves that such a multi-criteria decision support method is promising for the analysis and reduction of those risks, which are difficult to take into account by other methods of the decision-making and support, even in the case of merely three selection criteria with their contradictoriness, what takes place during the digitalization of the museum sphere. The ELECTRE I method is considered as a way to substantiate the choice of protective measures in terms of one of the principles of access control in relation to the digitized and newly produced copies of museum exhibits.

As a possible illustrative example of its application there are three criteria that are very important for the Museum and exhibition business when choosing one of the 2 most well-known principles for the access control to both the already created and still being created digital copies with delimited access: 1) average time of the intruder penetration into an automated system of the secure information processing; 2) time for the creation and disassembly of the museum exposition, taking into account the processes of authentication and authorization; 3) the cost of creating or modernizing the information security subsystem.

Keywords: information risks, alternatives, multi-criteria decision making, digital museum copies, protective measures

For citation: Sheptunov, M.V. (2020), “Applicability of the ELECTRE I method for multi-evaluating alternatives in tasks for selecting the access control principle to the museum digital copies”, *RSUH/RGGU Bulletin. “Information Science. Information Security. Mathematics” Series,* no. 4, pp. 62–71, DOI: 10.28995/2686-679X-2020-4-62-71

Введение и постановка задачи

Хотя ныне не вызывает сомнений важность резервного копирования файлов цифровых копий музейных и т. п. предметов, таковое лишь тогда может рассматриваться среди эффективных методов защиты от информационных рисков (в ракурсе, например, нарушения целостности цифровой музейной и/или архивной копии, ее подлинности, сохранности), когда оно входит в комплекс мероприятий достаточного уровня информационной безопасности всей совокупности копий того или иного музейного учреждения. Также существенно, что отсутствие одной либо большего количества данного вида копий рассматриваемого оригинала на момент произошедшего (как более распространенный вариант, страхового) случая его повреждения либо полной утраты чревато последствиями невозможности качественной реставрации и/или достоверного полного восстановления интересующего оригинала.

На аналогичное обстоятельство указывает, в т. ч., [Юмашева 2018] – создание электронной копии недостаточно с точки зрения обеспечения доступа к архивной информации; следующим необходимым этапом является разработка информационных ресурсов, чей функционал будет максимально адаптирован к запросам профессиональной исследовательской аудитории, работающей с архивными документами. Кроме того, в целом представляется, что в настоящий момент внедрение информационных технологий в практику архивного, библиотечного и музейного дела требует притока специалистов новой формации, имеющих два базовых образования – в области информации и той прикладной дисциплины, где предполагается использование ИТ.

Отметим в связи со сказанным, что не может не объединять специалистов этих двух областей столь важная для теории и практики учебная и научная дисциплина широкого охвата, как методы принятия (организационно-технических) решений (или, иначе называя, теория принятия решений), активно развивавшаяся в СССР совместно с социалистическими странами того времени, затем в России, в т. ч., академиком О.И. Ларичевым [Анич, Ларичев 1996], [Ларичев 2006].

И хотя при числе критериев до трех задача сравнения двух альтернатив нередко считается достаточно простой и прозрачной, но, во-первых, при большем количестве критериев задача становится малообозримой; во-вторых, упоминание о простоте и прозрачности более справедливо при отсутствии противоречивости (иначе говоря, разнонаправленности) 3-х критериев (что совершенно необязательно выполняется в задачах о выборе принципа управления доступом, особенно для музейной сферы); в-третьих, ситуация нередко еще усложняется при изменении предпочтений лица, принимающего решение (ЛПР) в процессе анализа проблемы, принятия им решения.

Здесь важно подчеркнуть методологическое отличие группы методов ELECTRE (Elimination Et Choix Traduisant la Realite – в переводе с французского в [Ларичев 2006] «исключение и выбор, отражающие реальность» или, иначе говоря – исключение и выбор в условиях реальности) – направленных на сравнение многокритериальных альтернатив – подхода РИПСА (Разработки Индексов Попарного Сравнения Альтернатив). Это основное отличие подхода французской школы принятия решений: в РИПСА предполагается формирование предпочтений лица, принимающего решение (ЛПР), в самом процессе анализа проблемы, осуществляемого с помощью метода принятия решений (что влечет за собой предъявление ЛПР самим методом различных вариантов решения проблемы в зависимости от решающих правил, воплощающихся в виде индексов попарного сравнения альтернатив). Таковое представляется особенно важным в случаях динамичных условий обстановки музейных и т.п. экспозиций и/или создания последних, включая как различные страховые случаи с частью экспонатов, так и нестраховые, с частью цифровых копий произведений искусства.

Основная часть

Рассмотрим применение упомянутого в заглавии метода ELECTRE I, который будем именовать, как и в [Ларичев 2006], подходом РИПСА (т. е. подходом, направленным на Разработку Индексов Попарного Сравнения Альтернатив). Напомним, что при подходе РИПСА понижаемое при первично несравнимых (при противоречивых критериях) альтернативах A_i, A_j значение уровня согласия α_1 и соответственно повышаемое значение уровня несогласия γ_1 до подходящих значений α и γ, при которых фактические значения этих уровней удовлетворяют соответственно неравенствам $C_{A_i A_j} \geq \alpha$ и $d_{A_i A_j} \leq \gamma$, при которых A_i оказывается превосходящей альтернативу A_j, предоставляют ЛПР (лицу, при-

нимающему решения) и консультанту (аналитику) инструмент исследования имеющегося множества альтернатив. Подчеркнем, что здесь сами предпочтения формируются в ходе анализа проблемы наряду с корректируемыми решающими правилами на основе индексов попарного сравнения альтернатив.

В нашем случае рассмотрим, например, ситуацию, когда при 3-х противоречивых критериях – выдвигаемых, например, экспертами – требуется выбрать между 2-мя принципиально важными альтернативами (считающимися взаимоисключающими). Допустим, такими тремя критериями являются:

1) среднее время проникновения злоумышленника в автоматизированную систему защищенной обработки информации (АСЗОИ),

2) время на создание и разборку музейной экспозиции с учетом процессов аутентификации и авторизации;

3) стоимость создания либо модернизации подсистемы защиты информации, причем их противоречивость в том, что упомянутое в первом критерии время должно быть максимальным при минимальном, упомянутом во 2-м критерии, времени на создание и разборку и при минимальной, упомянутой в 3-м критерии, стоимости создания.

Двумя возможными альтернативами, полагаемыми (для некоторого упрощения) взаимоисключающими (несовместными), и в рамках которых планируется дальнейшее уточнение соответствующих средств и методов защиты (совместно с создаваемыми к ним моделям угроз и/или моделям нарушителя), допустим, являются:

I) применение матричного (дискреционного) принципа управления доступом;

II) применение мандатного (полномочного) принципа управления доступом.

Хорошо известно, что каждый из этих принципов имеет свои достоинства и недостатки.

Предполагается, что создаваемая музейная экспозиция может быть комплексной, т. е. одна часть ее экспонатов материальна, а другая часть виртуальна (и может представляться дистанционно).

Допустим также, что имеет место следующий разброс оценок по критериям, представленный в табл. 1, а наиболее вероятные заданные кортежами значения оценок для альтернатив таковы:

A (5 мес., 4 дн., 3 тыс. евро),
B (6 мес., 3 дн., 4 тыс. евро),

причем веса вышеуказанных критериев: $w_1 = 3$, $w_2 = 2$, $w_3 = 1$.

Таблица 1

Нумерованное обозначение критерия	Критерий	Наихудшее значение	Наилучшее значение
$C_1 \equiv \bar{t}_1$	Среднее время проникновения злоумышленника в АСЗОИ	2 (мес.)	18 (мес.)
$C_2 \equiv t_2$	Время на создание и разборку музейной экспозиции с учетом процессов аутентификации и авторизации	8 (дн.)	1 (день)
$C_3 = S$	Стоимость создания либо модернизации подсистемы защиты информации	5 (тыс. евро)	2 (тыс. евро)

Тогда из представленных в табл. 1 данных условия примера имеем следующие длины шкал L_z (где $z = \overline{1,3}$):

$$L_1 = 18 - 2 = 16 \text{ (мес.)};$$
$$L_2 = 8 - 1 = 7 \text{ (дн.)};$$
$$L_3 = 5 - 2 = 3 \text{ (тыс. евро)}.$$

Вычисляя индексы согласия (с гипотезой о превосходстве альтернативы A_i над альтернативой A_j) как отношение суммы весов критериев подмножеств I^+ (подмножество критериев, по которым альтернатива A_i предпочтительнее альтернативы A_j) и $I^=$ (подмножество критериев, по которым A_i равноценна A_j) к общей сумме весов

$$C_{A_i A_j} = \frac{\sum\limits_{i \in I^+, I^=} w_i}{\sum\limits_{i=1}^{N} w_i} \qquad (1)$$

представим эти результаты в виде матрицы индексов согласия, сведенной в табл. 2: как ясно из условий данного примера, альтернатива A превосходит альтернативу B по одному 3-му критерию, т. к. 3 тыс. евро < 4 тыс. евро, и согласно формуле (1)

$$C_{AB} = \frac{w_3}{w_1 + w_2 + w_3} = \frac{1}{3+2+1} = \frac{1}{6} \approx 0{,}17;$$

альтернатива B превосходит альтернативу A по 2-м критериям (первому и 2-му), т. к.

6 мес. > 5 мес., 3 дн. < 4 дн., и согласно формуле (1)

$$C_{BA} = \frac{w_1 + w_2}{w_1 + w_2 + w_3} = \frac{3+2}{3+2+1} = \frac{5}{6} \approx 0{,}83.$$

Таблица 2

Индексы согласия для примера

Альтернатива	A	B
A	*	$\frac{1}{6} \approx 0{,}17$
B	$\frac{5}{6} \approx 0{,}83$	*

Вычисляемые далее индексы несогласия $d_{A_i A_j}$ (с гипотезой о превосходстве A_i над A_j) сведены в табл. 3, представленные в виде матрицы индексов несогласия при использовании формулы [Ларичев 2006]

$$d_{A_i A_j} = \max_{i \in I^-} \frac{l^i_{A_j} - l^i_{A_i}}{L_i}, \qquad (2)$$

где: $l^i_{A_i}$, $l^i_{A_j}$ – оценки альтернатив A_i и A_j по i-му критерию,

L_i – длина шкалы i-го критерия,

I^- – подмножество критериев, по которым A_j предпочтительнее A_i (или, при других обозначениях – подмножество критериев, по которым альтернатива B предпочтительнее альтернативы A).

Следует отметить, что, например, в [Петровский 2009] введен дополнительный уточняющий индекс l для каждого из имеющего отношение к формуле (2) (и, соответственно, формуле (1)) критерия, а сама формула (2) приведена в виде

$$d_{ij} = d(A_i, A_j) = \max_{l \in I^<_{ij}} (x_{jl} - x_{il}) / M, \qquad (3)$$

где $M = \max_l M_l$, $M_l = x_l^{max} - x_l^{min}$ – длина шкалы l-го критерия, равная максимальной разности оценок по этому критерию.

Для формирования табл. 3 используем формулу (2) с учетом уточнений, приведенных к ее аналогу (3):

$$d_{AB} = \frac{1дн.}{7дн.} = \frac{1}{7} \approx 0{,}14 \text{ (с учетом того, что}$$

$$max\left\{\frac{4дн.-3дн.}{8дн.-1дн.} = \frac{1}{7} \approx 0{,}14, \frac{6мес.-5мес.}{18мес.-2мес.} = \frac{1}{16} \approx 0{,}06\right\} = \frac{1}{7} \approx 0{,}14),$$

$$d_{BA} = \frac{4тыс.евро - 3тыс.евро}{5тыс.евро - 2тыс.евро} = \frac{1}{3} \approx 0{,}33.$$

Таблица 3

Индексы несогласия для примера

Альтернатива	*A*	*B*
A	*	$\frac{1}{7} \approx 0{,}14$
B	$\frac{1}{3} \approx 0{,}33$	*

Допустим, что ЛПР помощью консультанта задало (в итоге – при анализе проблемы в соответствии с подходом РИПСА) в качестве уровней согласия и несогласия соответственно: $\alpha_1 = \frac{1}{6}$ и $\gamma_1 = 0{,}15$.

Видно, с учетом данных табл. 2 и 3, что при этих уровнях α_1 и γ_1 альтернатива *A* превосходит альтернативу *B*. Учитывая смысловое содержание данного примера, этот вывод может означать, что даже несмотря на исходную более высокую важность (больший вес первого критерия) $w_1 = 3$ по сравнению с $w_2 = 2$ и более высокую важность этого же $w_1 = 3$ по сравнению с $w_3 = 1$, изначально несколько сомнительное превосходство альтернативы *A* над альтернативой *B* (но выясненное в ходе анализа проблемы при формировании предпочтений ЛПР наряду с корректируемыми решающими правилами с помощью консультанта либо аналитика)

объяснимо – как вариант – тем, что ЛПР мог(ло) решить предпочесть немного снизить затраты на создание либо модернизацию подсистемы защиты информации при допустимом небольшом увеличении окладов сотрудников службы безопасности организации. Указанная принятая ЛПР мера была бы способна если и не полностью, то частично компенсировать то, что по первому и 2-му критериям альтернатива *A* – хотя и не очень сильно – уступала альтернативе *B*.

Заключение

Научная новизна данной *статьи* заключается в следующем:

- выяснение возможности использования, по крайней мере, одного из методов ELECTRE (а именно ELECTRE I) – для задач информационной безопасности музейных цифровых копий и/или их коллекций;
- выяснение применимости метода ELECTRE I в качестве способа обоснования выбора защитных мер в ракурсе одного из принципов разграничения доступа в отношении оцифрованных и производимых цифровых копий музейных экспонатов.

Практическая ценность результатов в принципиальной и важной для приложений возможности использования метода для анализа и снижения различных информационных рисков музейной сферы, трудноучитываемых другими методами принятия и поддержки решений для задач многокритериального выбора защитных мер для ее электронных ресурсов.

Часть задач данной работы поставлена автором еще в период его деятельности в Финансовом университете и дополнена в ныне уточненном виде во время прохождения повышения квалификации в НИУ «ВШЭ» (Национальный исследовательский университет «Высшая Школа Экономики») и решена совместно с другой ее частью в нынешнем варианте во время работы и в ФГБОУ ВО «МГЛУ» (Московский Государственный лингвистический университет).

Литература

Анич, Ларичев 1996 – *Анич И., Ларичев О.И.* Метод ЭЛЕКТРА и проблема ацикличности отношений альтернатив // Автоматика и телемеханика. 1996. № 8. С. 108–118.

Ларичев 2006 – *Ларичев О.И.* Теория и методы принятия решений, а также Хроника событий в Волшебных странах. М.: Университетская книга, Логос, 2006.

Петровский 2009 – *Петровский А.Б.* Теория принятия решений. М.: Академия, 2009.

Юмашева 2018 – *Юмашева Ю.Ю.* Современные методы оцифровки объектов историко-культурного наследия как способы обеспечения их безопасности // Международный гуманитарный научный форум «Гуманитарные чтения РГГУ-2018 “Непрерывность и разрывы: Социально-гуманитарные измерения”». М.: Янус-К, 2018. С. 18–24.

References

Anich, I. and Larichev, O.I. (1996), “ELECTRA method and the issue of acyclicity in relations of alternatives”, *Automation and Remote Control*, vol. 57, no. 8, pp. 1154-1162.

Larichev, O.I. (2006), *Teoriya i metody prinyatiya reshenii, a takzhe Hronika sobytii v Volshebnyh stranakh* [Theory and methods of decision-making, as well as Chronicle of events in Magical countries], Universitetskaya kniga, Logos, Moscow, Russia.

Petrovskii, A.B. (2009), *Teoriya prinyatiya reshenii* [Decision theory], Akademiya, Moscow, Russia.

Yumasheva, Ju.Ju. (2018), “Modern methods for digitization of the historical-cultural heritage objects as methods to ensure their safety”, *Mezhdunarodnyi gumanitarnyi nauchnyi forum “Gumanitarnye chteniya RGGU-2018 ‘Nepreryvnost’ i razryvy: Sotsial’no-gumanitarnye izmereniya’”* [International humanitarian scientific forum “Humanitarian Conference of RSUH-2018 “Continuity and discontinuities. Social-humanitarian dimensions’”], Yanus-K, Moscow, Russia, 2018, pp. 18–24.

Информация об авторе

Максим В. Шептунов, кандидат технических наук, доцент, Российский государственный гуманитарный университет; 125993, Россия, г. Москва, Миусская пл., д. 6;

Московский государственный лингвистический университет; 119034, Россия, г. Москва, ул. Остоженка, д. 38/ 1; triumf403@yandex.ru

Information about the author

Maksim V. Sheptunov, Cand. of Sci. (Computer Science), associate professor, Russian State University for the Humanities, Moscow, Russia; bld. 6, Miusskaya Sq., Moscow, Russia, 125993;

Moscow State Linguistic University, Moscow, Russia; bld. 38/1, Ostozhenka Str., Moscow, Russia, 119034; triumf403@yandex.ru

Дизайн обложки
Е.В. Амосова

Корректор
Ж.П. Григорьева

Компьютерная верстка
М.Е. Заболотникова

Подписано в печать 15.12.2020.
Формат 60×90 1/16.
Уч.-изд. л. 4,3. Усл. печ. л. 4,5.
Тираж 1050 экз. Заказ № 1141

Издательский центр
Российского государственного
гуманитарного университета
125993, Москва, Миусская пл., 6
www.rggu.ru
www.knigirggu.ru