DOI 10.37882/2223–2966.2020.06.15

УГРОЗЫ ИНФОРМАЦИОННОГО ВОЗДЕЙСТВИЯ НА ИНФОРМАЦИОННЫЕ СИСТЕМЫ ОБРАЗОВАТЕЛЬНЫХ ОРГАНИЗАЦИЙ

Ивлиев Сергей Николаевич
К.т.н., доцент, ФГБОУ ВО «Национальный исследовательский Мордовский государственный университет имени Н. П. Огарева», Саранск
ivliev_ibis@mrsu.ru
Крылова Светлана Львовна
Старший преподаватель, ФГБОУ ВО «Национальный исследовательский Мордовский государственный университет имени Н. П. Огарева», Саранск
krilova_ibis@mrsu.ru
Квасков Алексей Александрович
Аспирант, ФГБОУ ВО «Национальный исследовательский Мордовский государственный университет имени Н. П. Огарева», Саранск
alexeikvaskov@yandex.ru

THREATS OF INFORMATION IMPACT ON INFORMATION SYSTEMS OF EDUCATIONAL INSTITUTIONS

S. Ivliev
S. Krylova
A. Kvaskov

Summary. Introduction: In educational organizations, the threat of information impact is of particular importance. Information systems used in the educational process, created without taking into account the requirements of information security, can have a significant number of vulnerabilities.

Materials and methods: On the basis of the analysis the most characteristic vulnerabilities of information systems of educational organizations are revealed, the model of threats of information educational environment is developed.

Results: studies have shown that the greatest effect of the information impact is achieved by the integrated use of methods of information technology and information psychological impact, to assess the danger of which a classification is proposed.

Discussion and Conclusions: On the basis of their studies proposed a minimum set of organizational and program-technical measures to counter the effects of the information on the information system of educational institutions, which is subject to further revision, refinement, detail and implementation.

Keywords: information educational environment, threat, vulnerability, information impact, hybrid war, security.

Аннотация. Введение: В образовательных организациях особое значение приобретает угроза информационного воздействия. Используемые в образовательном процессе информационные системы, созданные без учета требований обеспечения информационной безопасности, могут иметь значительное количество уязвимостей.

Материалы и методы: на основе анализа выявлены наиболее характерные уязвимости информационных систем образовательных организаций, разработана модель угроз информационной образовательной среды.

Результаты исследования: Исследования показали, что наибольший эффект от информационного воздействия достигается комплексным использованием методов информационно-технического и информационно-психологического воздействия, для оценки опасности которого предложена классификация.

Обсуждение и заключения: на основании проведенных исследований предложен минимальный набор организационных и программно-технических мероприятий по противодействию информационному воздействию на информационные системы образовательных организаций, который подлежит дальнейшей доработке, уточнению, детализации и последующему внедрению.

Ключевые слова: информационная образовательная среда, угроза, уязвимость, информационное воздействие, гибридная война, защищенность.

Введение

Доктриной информационной безопасности Российской Федерации от 5 декабря 2016 г. отмечается: «Расширяются масштабы использования специальными службами отдельных государств средств оказания информационно-психологического воздействия, направленного на дестабилизацию внутриполитической и социальной ситуации в различных регионах мира и приводящего к подрыву суверенитета и нарушению территориальной целостности других государств. В эту деятельность вовлекаются религиозные, этнические, правозащитные и иные организации, а также отдельные группы граждан, при этом широко используются возможности информационных технологий» [1]. В настоящее время в западной прессе обсуждаются вопросы противодействия современной России на информационном поле [12–20].

Особое значение указанная угроза информационного воздействия приобретает в образовательных организациях. Применение в образовательном процессе информационных систем, организованных в виде справочников и баз данных, например, электронная образовательная среда (ЭОС), созданных без учета требований обеспечения информационной безопасности могут иметь значительное количество уязвимостей.

Обзор литературы

Теоретическому исследованию угроз информационного воздействия на население в последнее время уделяется все большее внимание [2–6]. Предлагаются методики построения моделей угроз информационно-технического и информационно-психологического воздействий [7]. Учитывая огромное значение защиты от негативного информационного воздействия молодежи, следует отметить ряд работ, посвященных оценке защищенности информационных систем образовательных организаций [8–10]. Настоящая работа посвящена вопросам разработки модели угроз для информационно-справочных систем образовательных организаций высшего образования.

Как отмечалось выше, для достижения информационного превосходства могут быть использованы информационно-техническое (ИТВ) и информационно-психологическое (ИПВ) воздействия. Особую опасность представляет их комплексное использование. Наибольшую известность приобрели теории Джона Уордена и Джона Бойда, являющиеся идеологами и разработчиками стратегии современных войн и военных конфликтов [7,11].

Следует подчеркнуть, что гибридная война предполагает использование нападающей стороной скрытых форм нападения (диверсии на объектах инфраструктуры и жизнеобеспечения, поддержка повстанческих движений и т.д.). При этом наиболее эффективным средством ведения гибридной войны является информационная война, позволяющая добиться стратегических целей без прямого военного столкновения.

В обобщенном виде информационное воздействие в гибридной войне представлено на рисунке 1.

Как отмечают идеологи информационных войн: «Главной технологией войны в информационно-идеологическом пространстве является замещение базовых ментальных ценностей данного социума ценностной системой агрессора» [21,22]. Однако, отмечено, что прямой удар по центру управления достаточно трудная задача, да и вычислить его географическое местоположение часто не представляется возможным. Поэтому в настоящее время принята модель, представленная на рисунке 2. Диаграмма показывает, что часть защищаемых ресурсов, в частности, инфраструктура и производство размещается перед «линией фронта», или вне зон контроля вооруженных сил, т.е. вне контролируемой территории. Примером может служить размещение объектов производства на территории других государств. Причем, данная модель больше характеризует период военных действий. В случае мирного времени любой элемент атакуемого государства может располагаться вне контролируемой зоны, т.к. любое государство связано огромным количеством экономических и культурных связей с другими государствами и территориями.

С развитием информационно-коммуникационных технологий границы контролируемой зоны часто носят неявный характер. Например, информационные ресурсы, или их клоны, могут располагаться на серверах, расположенных за границей, что позволяет агрессору использовать их в своих интересах.

В последнее время все большее внимание уделяется защите населения от негативного воздействия глобальной информатизации. Правоохранительные органы выпускают огромное количество материалов, предостерегающих граждан от угроз, таящихся в глобальных информационных системах. Проводятся беседы и опросы, касающиеся информационной культуры граждан. Но на наш взгляд, явно недостаточное внимание уделяется защите собственных информационных ресурсов. Проблемам защиты информационных систем образовательных организаций посвящено данное исследование.

Материалы и методы

Особенностью информационных систем образовательных организаций является большой объем персо-

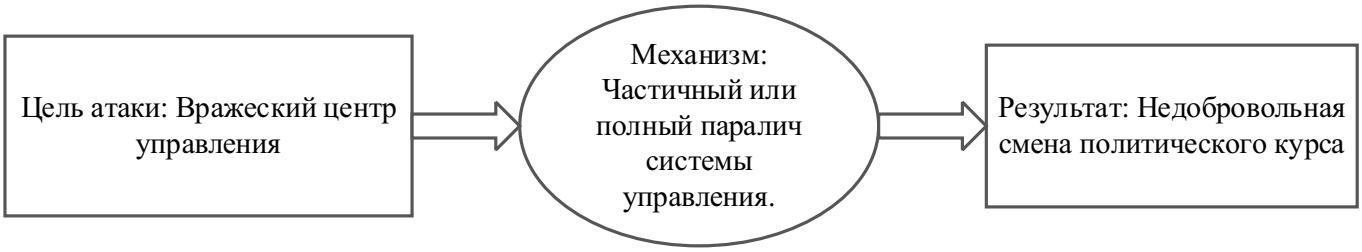

Рис. 1. Результат информационного воздействия в гибридной войне

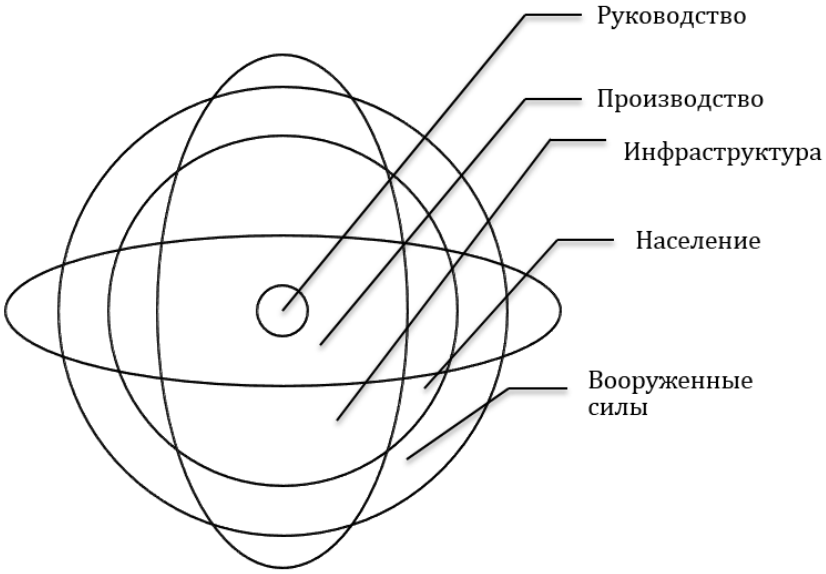

Рис. 2. Модифицированные кольца Бойда

нальных данных обучающихся, которые являются кадровым ресурсом государства. Ненадлежащее хранение и обработка этих данных позволяет агрессору посредством ИТВ на информационные ресурсы операторов персональных данных обучающихся, создавать базы данных и в дальнейшем проводить анализ с целью проведения ИПВ на субъекты, наиболее подверженные такому воздействию.

На основании исследования наиболее характерных уязвимостей информационных систем образовательных организаций была разработана модель угроз, представленная на рисунке 3.

В модели указаны наиболее характерные уязвимости информационных систем образовательных организаций. К ним относятся:

- Уязвимости в системном и прикладном программном обеспечении. Основным источником данной группы уязвимостей является использование программного обеспечения, не прошедшего процедуру подтверждения отсутствия недекларированных возможностей.
- Нарушение правил управления паролями и связанное с ним нарушение правил доступа к информации. Т.е. в большинстве образовательных организаций отсутствуют удостоверяющие центры. Регламентирующие документы, касающиеся порядка генерации распространения и утилизации паролей и прав доступа, в ряде случаев не соответствуют требованиям и рекомендациям регуляторов в области информационной безопасности.
- Использование сторонних почтовых сервисов создает предпосылки для несанкционированного обмена информацией. При этом резко повышается вероятность загрузки вредоносного кода.
- Использование для пересылки сообщений сервисов, предоставляемых социальными сетями и мессенджерами, так же открывает возможности для несанкционированного обмена информацией и внедрение вредоносного кода.

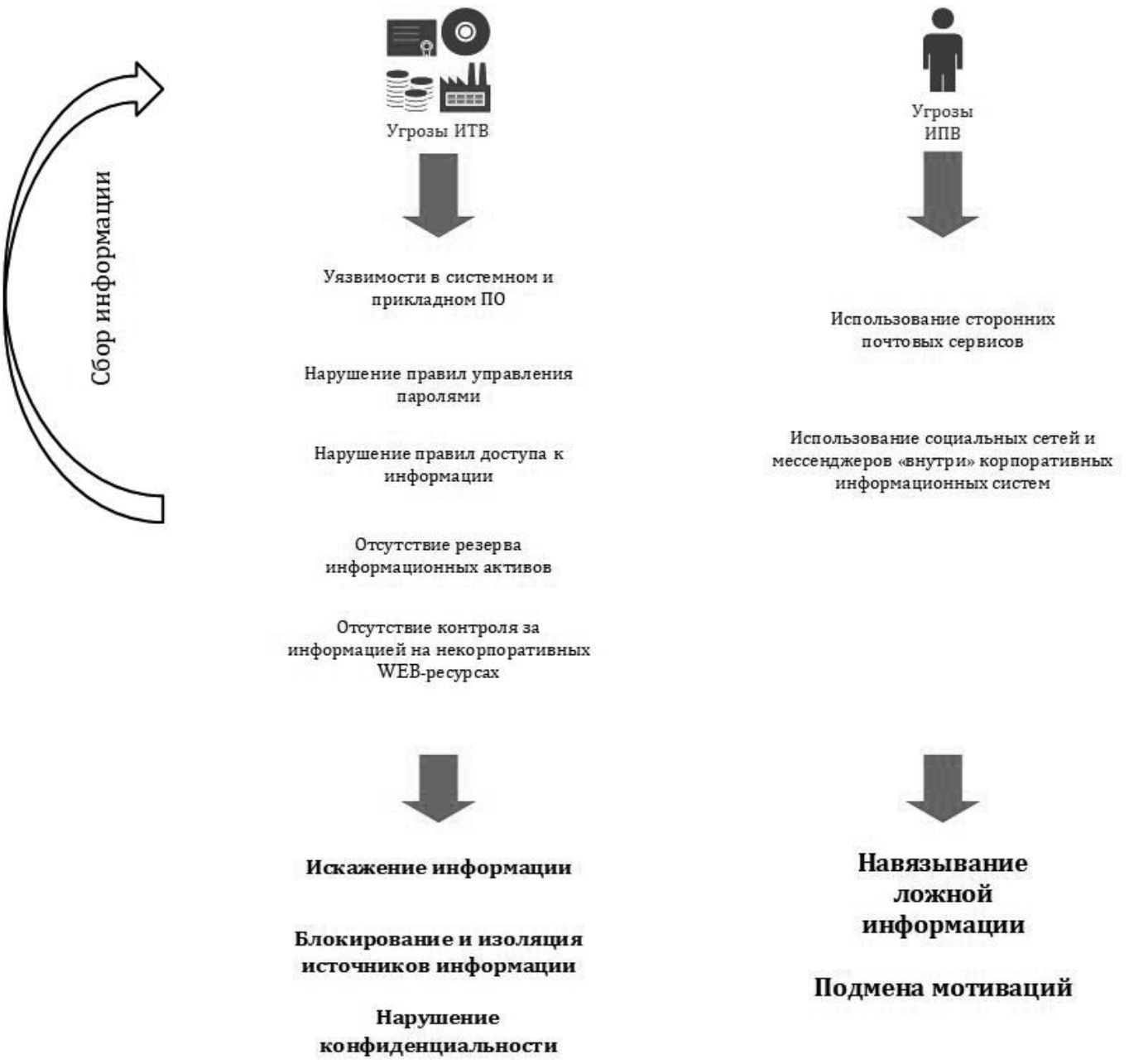

Рис. 3. Обобщенная модель угроз

- Использование собственных web-сайтов отдельных подразделений образовательного учреждения (чаще всего разработанных кустарно), не отвечающих требованиям безопасности, для несанкционированного, не контролируемого размещения внутренней (в том числе и конфиденциальной) информации на этих ресурсах.
- Отсутствие или малая эффективность системы периодического создания, обновления и хранения резервных копий информационных ресурсов.

Результаты исследования

Исследования показали, что наибольший эффект от информационного воздействия достигается комплексным использованием ИТВ и ИПВ. Для оценки опасности была принята следующая классификация:

- ИТВ, самостоятельно реализующие деструктивные функции на ИТКС и ИС и предназначенные для завоевания информационного противоборства. Они могут использоваться для доставки вредоносного кода или вредоносного контента.

- ИТВ, используемые для блокирования официальных источников информации.
- ИПВ, самостоятельно реализующие функции воздействия на личность, группы лиц, общество (фальсификация, дезинформация, дискредитация).
- ИПВ для «тандемного» усиления ущерба от ИТВ (например, требование оплаты за восстановление компьютера или данных после хакерской атаки).

При этом необходимо учитывать тот факт, что в информационном противоборстве преимущество получает нападающая сторона. Поэтому при оценке уязвимости информационных систем образовательных организаций в качестве исходных данных было принято наличие у атакующей стороны средств скрытого воздействия и проникновения в целевые информационные системы. Поэтому, мероприятия по информационной безопасности необходимо не только планировать при разработке технических заданий на информационные системы, но и в процессе сопровождения и модернизации указанных систем оценивать соответствие их требованиям нормативной документации в области информационной безопасности. А при изменении масштаба и структуры проводить их повторное категорирование и классификацию.

Обсуждение и заключения

На основании вышеизложенного, можно предложить следующий набор базовых организационных и программно-технических мероприятий по противодействию информационному воздействию на информационные системы образовательных организаций:

- Разработать пакет документов для внутреннего использования, отражающих основные положения, требования и правила обеспечения безопасности информационной системы (информационной образовательной среды) в соответствии законодательством РФ и рекомендациями регуляторов по ИБ. Осуществлять контроль сотрудников и обучающихся за выполнением установленных требований и правил.
- Использовать средства (сенсоры) предупреждения, обнаружения и ликвидации последствий информационно технического воздействия;
- Внедрить в практику эксплуатации информационных систем средства мониторинга несанкционированного воздействия на элементы информационных систем;
- Включить в структуры обслуживания корпоративных информационных систем образовательных организаций центры мониторинга и обработки данных по детектированию и предотвращению таргетированных атак на ресурсы информационных систем.

Разумеется, предложенный перечень мероприятий должен быть адаптирован (уточнен, конкретизирован и детализирован) для каждой конкретной образовательной организации с учетом целей, задач и специфики информационной образовательной среды на основе результатов анализа угроз и уязвимостей системы.

ЛИТЕРАТУРА

1. Доктрина информационной безопасности Российской Федерации (утв. Указом Президента Российской Федерации от 5 декабря 2016 г. № 646).
2. Макеев О. Ю. Информационное общество и угрозы информационных войн начала XXI века// Каспийский регион: политика, экономика, культура. 2013.— № 1 (34).— С. 132–139. URL: https://elibrary.ru/item.asp?id=18981962.
3. Зеленков М. Ю. Теоретико-методологические проблемы теории национальной безопасности Российской Федерации: Монография.— М. Юридический институт МИИТа, 2013.— 196 с.
4. Брянцева О. В. Развитие науки, технологий, образования как фактор национальной безопасности // Информационные технологии в юридической науке и образовании: сборник научных статей по материалам II Всероссийской научной конференции.— Саратов: Изд-во ФГБОУ ВО «Саратовская государственная юридическая академия», 2018.— С. 16–22. URL: https://elibrary.ru/item.asp?id=36492905.
5. Брянцева О.В., Брянцев И. И. Особенности реализации практик взаимодействия науки, образования и бизнеса в системе национальной безопасности // Вестник Поволжского института управления.— 2018.— Том 18.— № 4.— С. 4–13. URL: https://elibrary.ru/item.asp?id=36292668.
6. Брянцев И.И., Брянцева О. В. Влияние субъектов информационной сферы на устойчивость системы национальной безопасности к информационным войнам// Среднерусский вестник общественных наук, 2019.—Т. 14. № 1.— С. 203–217. URL: https://elibrary.ru/item.asp?id=37132098.
7. Антонов С.Г., Гордеев С. В., Климов С. М., Рыжов Б. С. Модели угроз совместных информационно-технических и информационно-психологических воздействий в гибридных войнах// Информационные войны, 2018.— № 2 (46).— С. 83–87. URL: https://elibrary.ru/item.asp?id=35078099.
8. Привалов А.Н., Гореликова Т. В. Информационная безопасность образовательных организаций в контексте информационных войн// Актуальные проблемы методики обучения информатике в современной школе Международная научно-практическая интернет-конференция. 2016 Из-во: Московский педагогический государственный университет (Москва).— С. 352–355. URL: https://elibrary.ru/item.asp?id=25694969.
9. Ивлиев С. Н. Предварительный анализ технической защищенности системы дистанционного образования (на материале Мордовского государственного университета) // Интеграция образования. 2012. № 4 (69). С. 27–31. URL: http://edumag.mrsu.ru/content/pdf/12–4.pdf.

10. Чиркова Т.Н., Крылова С. Л. Разработка электронного учебного ресурса в виртуальной обучающей среде MOODLE // Материалы XX научно-практической конференции молодых ученых, аспирантов и студентов Национального исследовательского Мордовского государственного университета им. Н. П. Огарёва в 3 ч.— 2016.— С. 288–292. URL: https://elibrary.ru/item.asp? id=27222009.
11. Савин Н. В. Пересмотр концепций «пяти стратегических колец» Дж. Уордена и «петли норд» Дж. Бойда// Информационные войны, 2015.— № 3 (35).— С. 44–51. URL: https://elibrary.ru/item.asp?id=35078099.
12. Garamone J. NATO commander Breedlove discusses implications of hybrid war // www.defense.gov/News-Article-View/Article/604334
13. Davis J. R. Continued evolution of hybrid threats URL: http://www.jwc.nato.int/images/stories/threeswords/CONTINUED_EVOLUTION_OF_HYBRID_THREATS.pdf
14. Gibbons-Neff T. The 'new' type of war that finally has the Pentagon attention URL: www.washingtonpost.com/world/national-security/the-new-type-of-war-that-finally-has-the-pentagons-attention/2015/07/03/ b5e3fcda-20be-11e5–84d5-eb37ee8eaa61_story.html? noredirect=on&utm_term=.b1ab57e102bb
15. Frank G. Hoffman. Conflict in the 21-th Century: the Rise of Hybrid Wars. Arlington, VA: Potomac Institute for Policy Studies, December 2007 URL: www.potomacinstitute.org/images/stories/publications/ potomac_hybridwar_0108.pdf.
16. Hybrid war — does it even exist? URL: NATO Review magazine URL: www.nato.int/docu/Review/2015/Also-in-2015/hybrid-modern-future-warfare-russia-ukraine/ EN/.
17. McGregor Knox and Williamson Murray, Eds. The dynamics of Military Revolution 1300–2050. Cambridge, Cambridge University Press, 2001. 36. Prashanth Parameswaran. Are We Prepared for 'Hybrid Warfare'? // The Diplomat. February 13, 2015 URL: thediplomat.com/2015/02/are-we-prepared-for-hybridwarfare/.
18. The US Army Operating Concept (AOC): Win in a Complex World 2020–2040. 7 October 2014 URL: www.tradoc.army.mil/ tpubs/pams/TP525–3–1.pdf.
19. Ferdinando L. Breedlove: Russia, instability threaten U.S., European security interests URL: www.defense.gov/News-Article-View/Article/673338/breedlove-russia-instability-threaten-us-european-security-interests
20. Davis J.R., Jr. The hybrid mindset and operationalizing innovation: toward a theory of hybrid URL: www.dtic.mil/dtic/tr/fulltext/u2/ a611901.pdf
21. Hoffman F. G. Conflict in the 21th Century: the Rise of Hybrid Wars. URL: www.potomacinstitute.org/images/stories/ publications/ potomac_hybridwar_0108.pdf
22. Hoffman F. G. Hybrid war — does it even exist? // NATO Review magazine. URL: www.nato.int/docu/Review/2015/Also-in-2015/hybrid-modern-future-warfare-russia-ukraine/EN

© Ивлиев Сергей Николаевич (ivliev_ibis@mrsu.ru),
Крылова Светлана Львовна (krilova_ibis@mrsu.ru), Кваскова Алексей Александрович (alexeikvaskov@yandex.ru).
Журнал «Современная наука: актуальные проблемы теории и практики»

Г. Саранск