РОССИЙСКАЯ АКАДЕМИЯ НАУК
ЦЕНТР ИССЛЕДОВАНИЯ ПРОБЛЕМ БЕЗОПАСНОСТИ
ИНСТИТУТ СОЦИАЛЬНО-ПОЛИТИЧЕСКИХ ИССЛЕДОВАНИЙ

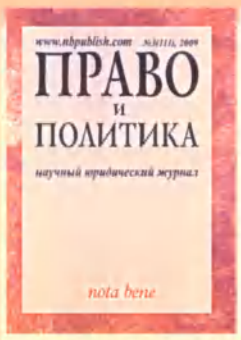
НАЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ

научный журнал

nota bene

№6 (29) июнь 2013 www.nbpublish.com

Издательство NOTA BENE представляет свои периодические издания.
Подписаться на все наши журналы можно с любого месяца. Индексы изданий размещены в Объединенном каталоге «ПРЕССА РОССИИ» (обложка зеленого цвета), который имеется во всех почтовых отделениях России и стран СНГ.

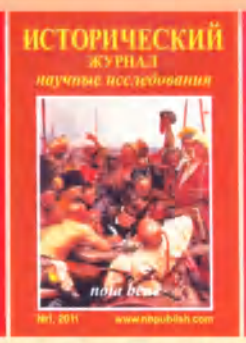


«Право и политика»
Ежемесячный, (объем и вес издания варьируются), формат А4, 248-278 стр., вес 600-700 гр.
Полугодовой индекс в «Прессе России» – **41896**

«Международное право и международные организации/ International Law and International Organizations»
Ежеквартальный, формат А4, 152 стр.
Полугодовой индекс в «Прессе России» – **82695**

«Журнал зарубежного законодательства и сравнительного правоведения»
Один раз в два месяца, формат А4, 120 стр., вес 260 гр.
Полугодовой индекс в «Прессе России» – **42274**

«Исторический журнал»
Ежемесячный, формат А4, 112 стр., вес 400 гр.
Полугодовой индекс в «Прессе России» – **41894**



«Исторический журнал: научные исследования»
Один раз в два месяца, формат А4, 120 стр., вес 260 гр.
Полугодовой индекс в «Прессе России» – **81948**

«Административное и муниципальное право»
Ежемесячный, формат А4, 100 стр., вес 260 гр.
Полугодовой индекс в «Прессе России» – **42279**

«Налоги и налогообложение»
Ежемесячный, формат А4, 80 стр., вес 160 гр.
Полугодовой индекс в «Прессе России» – **41895**

«Полицейская деятельность»
Ежеквартальный, формат А4, 100 стр, вес 220 гр.
Полугодовой индекс в «Прессе России» – **81937**

«Психология и психотехника»
Ежемесячный, формат А4, 100 стр., вес 220 гр.
Полугодовой индекс в «Прессе России» – **42278**

«Национальная безопасность/Nota bene»
Раз в два месяца, формат А4, 150 стр., вес 400 гр.
Полугодовой индекс в «Прессе России» – **81935**

«Философия и культура»
Ежемесячный, формат А4, 150 стр., вес 350 гр.
Полугодовой индекс в «Прессе России» – **42251**

«Актуальные проблемы российского права»
Ежемесячный, формат А4, 150 стр., вес 260 гр.
Полугодовой индекс в «Прессе России» – **11178**

«Культура и искусство»
Один раз в два месяца, формат А4, 120 стр., вес 260 гр.
Полугодовой индекс в «Прессе России» – **81908**

«Филология: научные исследования»
Ежеквартальный, формат А4, 100 стр., вес 160 гр.
Полугодовой индекс в «Прессе России» – **81909**

«Педагогика и просвещение»
Ежеквартальный, формат А4, вес 100 гр.

«Международные отношения»
Ежеквартальный, формат А4, 150 стр., вес. 350 гр.
Полугодовой индекс в «Прессе России» – **11181**

«Lex russica (Русский закон)»
Ежемесячный, формат А4, 150 стр., вес 350 гр.
Полугодовой индекс в «Прессе России» – **11198**

Программные системы и вычислительные методы
Ежеквартальный, формат А4, 150 стр., вес 355 гр.
Полугодовой индекс в «Прессе России» – **11183**

«Политика и общество»
Ежемесячный, формат А4, 150 стр., вес 400 гр.
Полугодовой индекс в «Прессе России» – **41897**

Тренды и управление
Ежеквартальный, формат А4, 150 стр., вес 350 гр.
Полугодовой индекс в «Прессе России» – **11920**

Подписаться можно и в альтернативных агентствах, работающих с нашим издательством:
«Интерпочта» – 500-00-60 (многоканальный), 921-33-10, 745-40-47. **«Артос-Гал»** – 795-23-00, 603-27-32, 603-27-31. **«МК-Периодика»** – 681-37-98, 681-57-15. **«Урал-Пресс»** – 257-08-13, 789-86-36 (а также есть отделения во всех регионах России). **«Орикон-М»** – 937-49-59. **«Дельта-пост»** – 261-33-72.

Издательство NOTA BENE впервые открывает подписку на электронные версии всех своих журналов. Доступ к нашим базам данных почти в два раза дешевле печатных изданий. Подписчик за одну подписку получает право доступа к изданиям с двух компьютеров. Возможно цитирование путем копирования.
Вниманию библиотек и корпоративных клиентов: при подписке на несколько электронных версий возможны дополнительные скидки.
Предлагаем подписку на блоки статей, сформированные по отраслям науки и интересам читателей, например: антропология, криминология, конституционное право, философия науки, история Древнего мира, история войн...

Наши научные журналы включены в перечень изданий, реферируемых Высшей аттестационной комиссией Министерства образования и науки РФ при присуждении докторских и кандидатских степеней. Подробнее смотрите на сайте www.nbpublish.com или на сайте ВАК

РОСИИЙСКАЯ АКАДЕМИЯ НАУК. ЦЕНТР ИССЛЕДОВАНИЯ ПРОБЛЕМ БЕЗОПАСНОСТИ, ИНСТИТУТ СОЦИАЛЬНО-ПОЛИТИЧЕСКИХ ИССЛЕДОВАНИЙ

НАЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ /NOTA BENE – №6(29) • 2013
(NATIONAL SECURITY /NOTA BENE)

Редакционный совет

Шульц Владимир Леопольдович – член-корреспондент Российской академии наук, заместитель президента Российской академии наук, доктор философских наук, директор Центра исследования проблем безопасности Российской академии наук, Председатель редакционного совета, шеф-редактор научного журнала «Национальная безопасность/notabene».119991, Россия, г. Москва, Ленинский проспект, 14;

Юрченко Александр Васильевич — директор Института проблем безопасности Национального исследовательского университета Высшая школа экономики, заместитель шеф-редактора научного журнала «Национальная безопасность/nota bene» 109028, Россия, г. Москва, Покровский бульвар, 11, офф. 227

Махутов Николай Андреевич – член-корреспондент Российской академии наук, заместитель академика-секретаря Отделения энергетики, машиностроения, механики и процессов управления Российской академии наук.119991, Россия, г. Москва, Ленинский проспект, 14;

Хабриева Талия Ярулловна – Вице-президент Российской академии наук, директор Института законодательства и сравнительного правоведения при Правительстве России. 117218, Россия, г. Москва, ул. Б.Черемушкинская, 34;

Юсупов Рафаэль Мидхатович – член-корреспондент Российской академии наук, директор Санкт-Петербургского института информатики и автоматизации Российской академии наук.199178, Россия, г. Санкт-Петербург,14 линия, дом 39;

Боярски Марек – доктор права, профессор, ректор Вроцлавского университета (Польша, г. Вроцлав).UniversityOfWroclaw, Pl. Uniwersytecki, 1, 50-137.Wrocław, Poland;

Гропп Вальтер – доктор права, профессор, руководитель профессуры, Юстус Либих – Университет Гиссен, (Германия, г. Гиссен).Raum 219, 2. Etage, LicherStraße, 76. 35394,Giessen, Deutschland;

Гирько Сергей Иванович – доктор юридических наук, профессор, начальник ВНИИ МВД Российской Федерации.123995, Россия, г. Москва, Г-69, ГСП-5, ул. Поварская, 25;

Дубовик Ольга Леонидовна – доктор юридических наук, профессор, главный научный сотрудник Института государства и права Российской академии наук. 119019, Россия, г. Москва, ул.Знаменка,10;

Зибер Ульрих – доктор права, профессор, директор Института зарубежного и международного уголовного права. Макса Планка, (Германия, г. Фрайбург).Günterstalstr., 73, 79100 Freiburgi. Breisgau,Deutschland;

Зинн Арндт – доктор права, профессор, руководитель Института экономического уголовного права Университета Оснабрюк, руководитель кафедры немецкого и европейского уголовного права и уголовного процесса, международного уголовного права и сравнительного правоведения (Германия, г. Оснабрюк). Universität Osnabrück, Postfach 44 69, 49069 Osnabrück, Deutschland;

Идрисов Рустам Фидайович – доктор юридических наук, профессор, главный Федеральный инспектор по Республике Татарстан. 420015, Россия, г. Казань, ул. К.Маркса, 61;

Хинрих Юлиус – доктор права, профессор юридического факультета Гамбургского университета, Центр „Юридический диалог с развивающимися странами" по исследованиям гражданского права и хозяйственного права, координатор проекта ЕС «China-EU SchoolofLaw». UniversitätHamburg, Mittelweg. 177. 20148,Hamburg, Deutschland.

Хэ Бинсун – доктор права, профессор, начальник Центра по изучению терроризма и организованной преступности, заместитель Начальника Центра по изучению уголовных законов, специальный консультант докторантов Политико-юридического университета Китая.100088, КНР, г. Пекин, район Хайдянь, Ул. Ситучэнлу д.25. (地址：北京市海淀区西土城路25号…)

Board of Editors

Schultz, Vladimir Leopoldovich – Corresponding Member of the Russian Academy of Sciences, Deputy President of the Russian Academy of Sciences, Doctor of Philosophy, Director of the Center for Security Studies of the Russian Academy of Sciences, Chairman of the Board of Editors, Editor-in-Chief of the Scientific Journal "National Security/nota bene». 119991, Russia, Moscow, Leninsky Prospect, 14

Yurchenko, Aleksandr Vasilievich – Director of the Institute of Security Problems of the National Research University – Higher School of Economics, Vice-Editor-in-Chief of the Scientific Journal "National Security/nota bene", 109028, Russia, Moskva, Pokrovsky bulvar, d.11 of. 227.

Makhutov, Nikolay Andreevich – Corresponding Member of the Russian Academy of Sciences, Vice-Secretary Academician of the Energetic Department, Mechanical Industry, Mechanics and Managing Processes of the Russian Academy of Sciences. 119991, Russia, Moscow, Leninsky Prospect, 14

Khabrieva, Talia Yarullovna – Vice-President at Russian Academy of Sciences, Director of the Institute of Legislation and Comparative Law under the Government of the Russian Federation. 117218, Russia, Moscow, ul. B.Cheremushkinskaya, 34

Yusupov, Rafael Midkhatovich – Correspondent Member of the Russian Academy of Sciences, Director of the St. Petersburg Institute for Information Sciences and Automation of the Russian Academy of Sciences. 199178, Russia, St. Petersburg, 14 line, 39

Boyarsky, Marek – Doctor of Law, Professor, Rector of the University Of Wroclaw (Wroclaw, Poland). University Of Wroclaw, Pl. Uniwersytecki, 1, 50-137. Wrocław, Poland

Gropp, Walter – Doctor of Law, Professor, Head of Professors, Justus Liebig Giessen University (Germany, Giessen). Raum 219, 2. Etage, Licher Straße, 76. 35394, Giessen, Deutschland;

Girko, Sergey Ivanovich – Doctor of Legal Sciences, Professor, Head of the All-Russian Scientific Research Institute of the Ministry of Internal Affairs of the Russian Federation. 123995, Russia, Moscow, G-69, GSP-5, ul. Povorskaya, 25

Dubovik, Olga Leonidovna – Doctor of Legal Sciences, Professor, Chief Scientific Researcher of the Institute of State and Law of the Russian Academy of Sciences. 119019, Russia, Moscow, ul. Znamenka, 10

Sieber Ulrich – Doctor of Law, Professor, Director of the Max Planck Institute of Foreign and International Criminal Law (Freiburg, Germany). Günterstal str., 73, 79100 Freiburg i. Breisgau, Deutschland

Arndt Sinn – Doctor of Law, Professor, Head of the Institute of Economic Criminal Law of the University of Osnabruck (Osnabruck, Germany), Head of the Department of German and European Criminal Law and criminal procedure, international criminal law and comparative law (Germany, Osnabrück). Universität Osnabrück, Postfach 44 69, 49069 Osnabrück, Deutschland

Idrisov, Rustam Fidaiovich – Doctor of Legal Sciences, Professor, Chief Federal Inspector in the Republic of Udmurtia. 420015, Russia, Kazan, ul. K.Marksa, 61

Heinrich, Julius – Doctor of Law, Professor of the Faculty of Law of the Hamburg University, Center of Legal Dialogue with the Developing States on studies of civil and economic law, Coordinator of the EU Project "China-EU School of Law". Universität Hamburg, Mittelweg. 177. 20148, Hamburg, Deutschland.

He Bingsong – Doctor of Law, Professor, Head of the Center on Studies of Terrorism and Organized Crime, Aide to the Head of the Center for the Studies of Criminal Law, Special Consultant of the Doctoral Students of the Political and Legal University of China. 100088, Peoples Republic of China, Beijing, Haidian District, st. Situchenlu d.25. (地址：北京市海淀区西土城路25号…)

© NOTA BENE (ООО «НБ-Медиа») www.nbpublish.com

СОДЕРЖАНИЕ

ДОКТРИНА

Ахатов Ю. К.
Перспективные направления совершенствования социального управления процессами трудовой миграцией в Сахалинской области 4

Киреева Н. В.
О системном подходе к определению основных категорий общей теории безопасности 11

СТРАТЕГИЯ ОБЕСПЕЧЕНИЯ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

Данилов А. П.
Военный аспект арктической политики России 27

ГЛОБАЛИЗАЦИЯ И НАЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ

Андреев М. В.
Стратегии развития межкультурного диалога в контексте укрепления национальной безопасности: актуальные проблемы общественно-политической доктрины Западной Европы и США 35

ФАКТОР НАДЕЖНОСТИ В СИСТЕМАХ БЕЗОПАСНОСТИ

Царегородцев А. В., Ермошкин Г. Н.
Модель оценки рисков информационной безопасности информационных систем на основе облачных вычислений 46

ПРАВОВОЕ ОБЕСПЕЧЕНИЕ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

Дундуков М. Ю.
Правовая регламентация тайных операций разведки США 55

Демидов В.Н.
Вопросы национальной безопасности в деятельности органов Конституционной Юстиции в Российской Федерации 66

ВНУТРЕННИЙ КОНТУР НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

Чирков Д. К., Евланова О. А., Коимшиди Г. Ф.
Региональные особенности и различия преступлений в сфере незаконного оборота наркотиков 77

ВНУТРЕННИЕ УГРОЗЫ И КОНТРМЕРЫ

Пащенко И. В.
Глобальный Индекс Терроризма и ситуация на Северном Кавказе: мировые тенденции и региональные особенности 94

ВНЕШНИЙ КОНТУР НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

Карпович О. Г.
Некоторые особенности внешнеполитических отношений США и Венесуэлы на современном этапе 105

ВНЕШНИЕ УГРОЗЫ И ПРОТИВОДЕЙСТВИЕ

Евсеев В. В.
Сирийский кризис под углом российско-американских отношений 111

ЭКОНОМИЧЕСКОЕ ОБЕСПЕЧЕНИЕ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

Гой В. В.
Формирование специализированной институциональной системы управления сферой несостоятельности субъектов хозяйствования Украины 122

ГУМАНИТАРНОЕ ОБЕСПЕЧЕНИЕ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

Малинина К. О.
Механизм формирования социальной аномии 134

ЧЕЛОВЕК И ГРАЖДАНИН В СИСТЕМЕ БЕЗОПАСНОСТИ

Погонцева Д. В.
Этно-лукизм: взгляд на проблему 144

НАУЧНАЯ ЖИЗНЬ

Черкасов В. Н.
Можно ли все-таки подсчитать рейтинг? (Размышления о монографии Ю. А. Шумилова. Введение в юридическую наукометрию) 151

SUMMARY 161

СВЕДЕНИЯ ОБ АВТОРАХ 168

ABOUT THE AUTHORS 171

CONTENTS

DOCTRINE
Akhatov, Y.K.
Perspective directions for the improvement of social administration of labor migration in the Sakhalin region 4

Kireeva, N.V.
On systemic approach to defining the main categories of the general security theory..... 11

STRATEGY OF NATIONAL SECURITY GUARANTEES
Danilov, A.P.
The military aspect of the Arctic policy of Russia..... 27

GLOBALIZATION AND NATIONAL SECURITY
Andreev, M.V.
Strategies for the development of inter-cultural dialog within the framework of strengthening national security: topical problems of social and political doctrine of the Western Europe and the USA 35

RELIABILITY FACTOR IN SECURITY SYSTEMS
Tsaregorodtsev, A.V., Ermoshkin, G.N.
The model for the evaluation of information security risks in the information system based upon the cloud computing..... 46

LEGAL GUARANTEES OF NATIONAL SECURITY
Dundukov, M.Y.
Legal regulation of secret intelligence operations of the USA..... 55

Demidov, V.N.
National security issues in the activities of the constitutional justice bodies in the Russian Federation..... 66

INNER CONTOUR OF NATIONAL SECURITY
Chirkov, D.K., Evlanova, O.A., Koimshidi, G.F.
Regional specific and distinguishing features of crimes in the sphere of illegal turnover of narcotic substances 77

INNER THREATS AND COUNTERMEASURES
Paschenko, I.V.
The Global Terrorism Index and the situation in the Northern Caucasian region: the global tendencies and regional specificities..... 94

OUTER CONTOUR OF NATIONAL SECURITY
Karpovich, O.G.
Some specific features of the current foreign political relations between the USA and Venezuela 105

OUTER THREATS AND COUNTERACTION
Evseev, V.V.
The Syrian crisis from the standpoint of Russian-American relations 111

ECONOMIC GUARANTEES OF NATIONAL SECURITY
Goy, V.V.
Formation of a specialized institutional system for managing the insolvency of economic subjects in Ukraine..... 122

HUMANITARIAN GUARANTEES OF NATIONAL SECURITY
Malinina, K.O.
Mechanism for the formation of social anomia 134

INDIVIDUAL AND CITIZEN WITHIN SECURITY SYSTEM
Pogontseva, D.V.
Etho-lookism: a glance at the problem 144

SCIENTIFIC LIFE
Cherkasov, V.N.
Is it still possible to establish the rating?
(Some thoughts on the monograph by Y.A. Shumilov. Introduction into legal scientometrics..... 151

SUMMARY 161

ABOUT THE AUTHORS (RUSSIAN) 168

ABOUT THE AUTHORS (ENGLISH)..... 171

DOI: 10.7256/2073-8560.2013.6.9585

Царегородцев А. В., Ермошкин Г. Н.

МОДЕЛЬ ОЦЕНКИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ НА ОСНОВЕ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

Аннотация. *Являясь одной из самых привлекательных современных информационных технологий, облачные сервисы могут, как оптимизировать процессы управления информационной безопасностью, так и усложнить для организации контроль над критичными данными и соблюдением контрмер на инциденты безопасности.Решение проблемы своевременного и качественного анализа рисков аутсорсинга информационной безопасности систем облачной архитектуры позволит решить множество проблем связанных с защитой от угроз использования информационных и телекоммуникационных технологий в противоправных целях. Широкое распространение и применение облачных вычислений диктует необходимость адаптации и доработки существующих моделей оценки рисков информационных систем. Подход, предлагаемый в статье, может быть использован для оценки рисков информационных систем, функционирующих на основе технологии облачных вычислений, и оценки эффективности принимаемых мер безопасности. При этом, оценка риска включает этапы анализа и оценивания, а анализ риска, в свою очередь, включает идентификацию и количественную оценку риска. Обеспечение оценки производится на основе определения контекста риска (выбора критериев риска и определения границ анализа). Под количественной оценкой риска понимается процесс моделирования, включающий разработку и анализ альтернативных сценариев риска, построение функций риска и определение вероятности его наступления.*

Ключевые слова: *информационная безопасность, облачные вычисления, публичное облако, частное облако, гибридное облако, оценка риска, риск-модель, матрица воздействий, матрица потерь, матрица зависимости.*

Введение

Являясь одной из самых привлекательных современных информационных технологий, облачные сервисы могут, как оптимизировать процессы управления информационной безопасностью, так и усложнить для организации контроль над критичными данными и соблюдением контрмер на инциденты безопасности.

Решение проблемы своевременного и качественного анализа рисков аутсорсин-

Все права принадлежат издательству © NOTA BENE (ООО «НБ-Медиа») www.nbpublish.com

DOI: 10.7256/2073-8560.2013.6.9585

га информационной безопасности систем облачной архитектуры позволит решить множество проблем связанных с защитой от угроз использования информационных и телекоммуникационных технологий в противоправных целях.

Анализ существующих моделей оценки риска является основой для разработки новой модели на современном наборе стандартов с учетом особенностей национальной специфики необходимой для создания концепции обеспечения ИБ при заключении договора аутсорсинга и для поддержания уровня риска на приемлемом уровне.

Оценка рисков на качественном уровне не позволяет однозначно сравнить затраты на обеспечение ИБ и получаемую от них отдачу (в виде снижения суммарного риска). Поэтому более предпочтительными представляются количественные методики. Но они требуют наличия оценок вероятности возникновения для каждой из рассматриваемых угроз безопасности. Кроме того, использование интегральных показателей, таких как ALE, опасно тем, что неправильная оценка вероятности угрозы в отношении очень дорогостоящего актива может кардинально изменить оцениваемое значение суммарной стоимости рисков.

В работе представлен анализ теоретических и научно-практических методов оценки риска для сложных технических систем. При этом, оценка риска включает этапы анализа и оценивания, аанализ риска, в свою очередь, включает идентификацию и количественную оценку риска. Обеспечение оценки производится на основе определения контекста риска (выбора критериев риска и определения границ анализа). Под количественной оценкой риска будем понимать процесс моделирования, включающий разработку и анализ альтернативных сценариев риска, построение функций риска и определение вероятности его наступления.

1. Определение зависимостей и атрибутов безопасности

Большинство проблем с безопасностью, так или иначе, связанно с вредоносным воздействием. Проблема здесь в первую очередь связанна с невозможностью верно измерить все факторы, а если нельзя все верно рассчитать, то и управлять результатом не получится.

Таким образом, первостепенной задачей становится создание инструментария для ведения правильных и своевременных расчетов. Вычислив все возможные ошибки и потери системы от них мы получим возможность провести расчеты необходимых контрмер и оценить результат их применения.

Существует ряд моделей подходящих для решения данной задачи. В этих моделях для определения надежности системы используютсяследующие показатели:

- ***Наработка на отказ (MTTF)*** — это продолжительность работы системы до момента появления первого сбоя. Данный параметр измеряется как: количество часов работы без сбоя всех устройств деленное на количество устройств.
- ***Среднее время между отказами (MTBF)*** — описывает среднее время работы системы между двумя последовательными сбоями (применяется для систем подлежащих восстановлению). Измеряется как все время работы системы, в часах разделенное на количество отказов.
- ***Наработка до обнаружения (MTTD)*** — описывает время между обнаружением ранее неизвестных уязвимостей системы.
- ***Наработка до отказа (MTTE)*** — отражает время работы системы до момента возникновения ошибки или использования уязвимости известные ранее.

Все права принадлежат издательству © NOTA BENE (ООО «НБ-Медиа») www.nbpublish.com

DOI: 10.7256/2073-8560.2013.6.9585

- ***Среднее доступное время работы*** — показатель времени в процессе работы системы, когда она доступна для использования.

Эти модели в том или ином виде отражают вероятность отказа всей системы, игнорируя различные особенности и начальное состояние систем, в т.ч. неравномерное распределение угроз, разницу в условиях возникновения ошибок и т.д.

В тоже время, например для оценки наработки системы на отказ, необходимо лишь смоделировать вероятности ошибок в соответствии с их спецификациями.

Чтобы использовать данные модели для решения задачи анализа рисков аутсорсинга информационной безопасности систем облачной архитектуры следует учесть следующие факторы:

- разницу в стоимости ошибки в зависимости от условия возникновения;
- разницу в вероятности возникновения сбоя для разных компонентов системы;
- разницу в результате возникновения ошибки для заинтересованных сторон.

В данной статье предлагается модель, в которой мы постарались учестьвсе вышеперечисленные факторы. Применение данной модели может способствовать рационализации принятия решений в системах облачных вычислений, тем самым способствовать сокращению издержек пользователей.

2. Модель оценки рисков

Распределенные информационно-вычислительные системы характеризуются пятью фундаментальными свойствами: функциональностью, мощностью, доступностью, стоимостью, надежностью. При этом, надежность будет включать и угрозы, и атрибуты, и средства её достижения.Несмотря на то, что существует ряд моделей позволяющих оценить надежность системы по таким показателям, как MTTF для выяснения отказоустойчивостии, MTTE для измерения уязвимостей системы, не существует способа измерить надежность напрямую или дать количественную оценку рискам безопасности.

Но, как показывает практика, не всегда возможно и нужно стараться учесть все существующие разновидности рисков. Так в большинстве случаев достаточно учитывать лишь риски, имеющие финансовую составляющую. Для их оценки в большей степени подходят количественные методы оценки.

В этом контексте предлагаемыйподход обладает рядом преимуществ:

- предлагаются данные о цене потерь: измеряя цену как количество финансовых потерь на единицу времени работы системы;
- проводятся измерения результатов ошибок: предоставляя количественный результат (цену) ошибок безопасности;
- предоставляются данные о потерях рассчитанные для различных заинтересованных сторон.

Матрица потерь

Пусть S — система, а $H_1, H_2, \ldots, H_k$ заинтересованные стороны. $R_1, R_2, \ldots, R_n$ требования безопасности в системе. $ST_{i,j}$, где$1 \le i \le k$, $1 \le j \le n$, стоимость потерь для стороны H_i в результате невыполнения требований безопасности R_j в зависимости от сегмента распределенной архитектуры, находящегося в управлении заинтересованной стороны H_i. PR_j где $1 \le j \le n$, вероятность, что система не соотносится с требованиями безопасности R_j, и MFC_i где $1 \le i \le k$ переменная отражающая стоимость потерь для стороны H_i в случае нарушения безопасности. Величина MFC измеряется в финансовых потерях на единицу операционного времени:

$$MFC_i = \sum_{1 \le j \le n} ST_{i,j} * PR_j.$$

Все права принадлежат издательству © NOTA BENE (ООО «НБ-Медиа») www.nbpublish.com

DOI: 10.7256/2073-8560.2013.6.9585

Пусть *MFC* вектор размерности *k* представляющий основные издержки в случаи нарушения требований безопасности, *PR* вектор размера *n* вероятность невыполнения требований безопасности и *ST* матрица $k \times n$ отражающая стоимость потерь в результате невыполнения требований безопасности, тогдаможно записать как произведение матриц:

$MFC = ST * PR$.

Матрица зависимостей

Пусть C_1, C_2, …, C_n — компоненты системы *S*. В зависимости от того какие из этих элементов функционируют будут выполнятся или не выполнятся требования безопасности. Если предположить, что возможен отказ лишь одного компонента системы, тогда можно ввести следующие события:

- E_i — событие при котором компонент C_i перестал функционировать в результате нарушения безопасности ($1 \leq i \leq h$).
- E_{m+i} — не один из компонентов не затронут.

Определив набор событий E_iможно записать вероятность наступления события *F* как: $P(F) = \sum_{k=1}^{h+1} P(F|E_k) * P(E_k)$.

Считаем что *F* — это событие, при котором не выполняется условие *R*, тогда:

$PR_j = \sum_{j=1}^{m+1} P(F_j|E_k) * P(E_k)$.

Здесь *DP*– матрица размерности$n \times h + 1$,строки *j* и столбцы *k* отражают вероятность отказа системы в случае, если компонент *k* не выполнил требование *j*. Введем вектор *PE* размерности *h*+1, т.к. PE_k– вероятность события E_k, тогда: $PR = DP * PE$.

Матрица заполняется в соответствии с существующими данными об архитектуре системы.

Матрица воздействий

Компоненты архитектуры могут перестать правильно функционировать в результате нарушения безопасности, вызванного вредоносным воздействием. Для этого определимпотенциальный набор угроз.

Пусть $T_1, T_2 \ldots, T_p$– реализовавшиеся угрозы, а T_{p+1}– не реализовавшиеся угрозы. Вектор *PT* размерности *p+1* представляет собой:

- PT_q — вероятность того, что угроза T_q реализовалась в процессе работы ($1 \leq q \leq p$).
- PT_{p+1} — вероятность того, что ни одна угроза не реализовалась в процессе работы.

Тогда получим:$PE_k = \sum_{q=1}^{p+1} P(E_k|T_q) * PT_q$.

Пусть *IM* — матрица воздействий размерности $h + 1 \times p + 1$, где строки *k* и столбцы *q* отражают вероятность того, что компонент C_k отказал в связи с реализацией угрозы T_q (или того, что угрозы не реализовались).

PT — вектор размерности $p + 1$, PT_q– вероятность того, что угроза T_q реализовалась. Тогда $PE = IM * PT$.

Матрица заполняется в соответствии с возможными угрозами и оценками вероятности их появления. *PT* заполняется, исходя из возможного поведения нарушителей, особенностей системы, подверженности угрозам и т.д.

В результате, исходя из полученных матриц и вектора угроз, получим вектор *MFC*:

$MFC = ST * DP * IM * PT$.

3. Применение модели оценки рисков для систем облачной архитектуры

Рассмотрим возможность применения разработанной риск-модели для систем облачной архитектуры. Для этого необходимо определить существующие требования безопасности, заинтересованные стороны и их участие в этих требованиях и архитектурных компонентах системы.

Матрица потерь

Будем считать, что основными требованиями безопасности для систем, функционирующих на основе технологии облачных вычислений (ОВ) являются: доступность, полнота и конфиденциальность. Рассмотрим эти требо-

Все права принадлежат издательству © NOTA BENE (ООО «НБ-Медиа») www.nbpublish.com

DOI: 10.7256/2073-8560.2013.6.9585

Таблица 1. Матрица потерь: стоимость потерь в результате невыполнения требований безопасности (тыс. долларов/час)

Заинтересованные стороны	Требования безопасности						
	ДКД	ДАД	ПКД	ПАД	КСД	КЧД	КПД
ПР	500	90	800	150	1500	1200	120
КК	150	40	220	80	250	180	60
ГК	60	20	120	50	2500	30	12
ИК	0,05	0,015	0,30	0,20	0,30	0,10	0,01

вания с учетом различного уровня важности данных, для которых они применяются.

Доступность: возможность пользователя получить доступ к своей информации в момент, когда она ему будет необходима. Недоступность данных может быть более или менее затратной в зависимости от важности данных для пользователя. Мы будем разделять их на две категории: критические и архивные данные.

Полнота: показывает, что данные пользователя защищены от потерь или повреждения в результате вредоносного воздействия или непредусмотренных действий. Нарушение полноты может иметь различные последствия и быть более или менее затратным в зависимости от важности данных для пользователя.Выделим две категории: для критичных и для архивных данных.

Конфиденциальность: показывает, что данные пользователя защищены от несанкционированного доступа. Нарушение конфиденциальности может принести больше или меньше потерь пользователю в зависимости от уровня их конфиденциальности. Данные могут быть разделены на три категории: секретные, частные, публичные.

Для данной модели будем предполагать, что мы имеем дело с семью требованиями безопасности:

- ДКД: доступность к критическим данным.
- ДАД: доступность к архивным данным.
- ПКД: полнотакритических данных.
- ПАД: полнотаархивных данных.
- КСД: конфиденциальность секретных данных.
- КЧД: конфиденциальность частных данных.
- КПД: конфиденциальность публичных данных.

Будем считать, что провайдер услуг принимает в расчет важность данных и устанавливает приоритет выполнения более важных требований. Также будем считать, что все клиенты обладают равными правами и их данные защищаются одинаково, таким образом, если провайдер не может обеспечить выполнение определенных требований безопасности, то данная угроза распространяется для всех пользователей.

Для систем ОВ существует три класса заинтересованных сторон: провайдер услуг, корпорации или организации (юридические лица), индивидуальные пользователи (физические лица).

Пусть мы имеем дело с провайдером (ПР) и тремя клиентами: корпоративным клиентом (КК), государственным клиентом (ГК), индивидуальным клиентом (ИК).

В табл. 1 показаны потери заинтересованных сторон, рассчитанные в тыс. долларов на час операционного времени.

Матрица зависимости

Благодаря виртуализации системы ОВ оптимизируют затраты на ресурсы, позволяя пользователям использовать множество

Все права принадлежат издательству © NOTA BENE (ООО «НБ-Медиа») www.nbpublish.com

DOI: 10.7256/2073-8560.2013.6.9585

Таблица 2. Матрица зависимости

Требования безопасности	Компоненты									
	Браузер	Прокси сервер	Роутер/ МЭ	Загрузочный балансировщик	Веб сервер	Сервер приложений	БД	Сервер резервного копирования	Сервер хранения	Нет сбоев
ДКД	1	1	1	1	0,44	0,28	1	0,01	1	0
ДАД	1	1	1	1	0,44	0,28	0,28	0,01	1	0
ПКД	0,14	0,14	1	1	0,44	0,14	1	0,01	1	0
ПАД	0,14	0,14	1	1	0,44	0,14	0,14	0,01	1	0
КСД	0,44	0,14	1	1	0,44	0,44	0,44	0,01	0,44	0
КЧД	0,44	0,14	1	1	0,44	0,44	0,44	0,01	0,44	0
КПД	0,44	0,14	1	1	0,44	0,44	0,44	0,01	0,44	0

Угрозы	
МВМ	Мониторинг виртуальной машины
КВМ	Коммуникации между ВМ и хостом
МодМВ	Модификация (изменение) ВМ
ВВМ	Размещение вредоносного образа ВМ в физической системе
МДВМ	Мониторинг ВМ другими ВМ
КМВМ	Коммуникации между ВМ
МобВМ	Мобильность ВМ
DoS	Отказ в обслуживании
FA	Flooding attacks (флуд атаки)
ПД	Потеря, кража данных
ВА	Внутренние агенты
КАУТ	Кража аккаунта, трафика, услуг
НПП	Нарушение правил пользования
НПИ	Небезопасный программный интерфейс
Нет	Нет угроз

Таблица 3. Матрица воздействий

Компоненты	Угрозы														
	МВМ	КВМ	МодМВ	ВВМ	МДВМ	КМВМ	МобВМ	DoS	FA	ПД	ВА	КАУТ	НПП	НПИ	нет
Браузер	0	0	0	0	0	0	0	0,02	0,01	0	0,03	0,02	0	0,03	0
Прокси	0,01	0,05	0	0,01	0,01	0,05	0,05	0,02	0,01	0	0,005	0,02	0,01	0	0
Р/ФВ	0,03	0,05	0,033	0,03	0,03	0,05	0,05	0,06	0,04	0	0,005	0,02	0,01	0,01	0
Балансировщик	0,02	0,003	0	0,01	0,02	0,003	0,003	0,06	0,04	0	0,005	0,02	0,01	0,01	0
Веб сервер	0,03	0,003	0,033	0	0,03	0,003	0,003	0,02	0,04	0	0,01	0,02	0,01	0,01	0
Прил. сераер	0,02	0,003	0,033	0,06	0,02	0,003	0,003	0,036	0,04	0	0,05	0,02	0,01	0,07	0
БД	0,001	0	0,033	0,04	0,001	0	0	0,036	0,04	0,05	0,03	0,02	0,01	0,06	0
Бекап сервер	0,001	0	0	0,04	0,001	0	0	0,036	0,04	0,05	0,03	0,02	0,01	0,06	0
Хранилище	0,04	0,05	0	0,04	0,04	0,05	0,05	0,036	0,04	0,05	0,03	0,02	0,01	0,06	0
Нет сбоев	0,06	0,04	0,03	0,03	0,06	0,04	0,04	0,01	0, 02	0,01	0,02	0,05	0,06	0,005	1

Все права принадлежат издательству © NOTA BENE (ООО «НБ-Медиа») www.nbpublish.com

DOI: 10.7256/2073-8560.2013.6.9585

Таблица 4. Вектор угроз

Угрозы	Вероятность
МВМ	$8{,}063*10^{-4}$
КВМ	$8{,}063*10^{-4}$
МодМВ	$8{,}063*10^{-4}$
ВВМ	$8{,}063*10^{-4}$
МДВМ	$40{,}31*10^{-4}$
КМВМ	$40{,}31*10^{-4}$
МобВМ	$40{,}31*10^{-4}$
DoS	$14{,}39*10^{-4}$
FA	$56{,}44*10^{-4}$
Угрозы	**Вероятность**
ПД	$5{,}75*10^{-4}$
ВА	$6{,}623*10^{-4}$
КАУТ	$17{,}277*10^{-4}$
НПП	$17{,}277*10^{-4}$
НПИ	$29{,}026*10^{-4}$
нет	0,9682

Таблица 5. Стоимость потерь для заинтересованных сторон

Заинтересованные стороны	Стоимость
ПР	15,20443
КК	3,53839
ГК	8,98502
ИК	0,00341

приложений и функций на одном, а не на множестве устройств. Рассмотрим уровневую организацию ОВ:

- базовые составляющие: браузер, прокси-сервер, роутер, межсетевой экран (МЭ) и загрузочный балансировщик;
- облачные сервисы: веб сервер, сервер приложений, база данных, сервер хранения и восстановления информации;
- пользовательские инструменты.

Предположим, что за раз происходит сбой лишь одного компонента и, учитывая случай, когда все компоненты работают, построим матрицу.

Матрица воздействий

Следующий шаг — это построение матрицы воздействий. Системы ОВ подвержены множеству типов угроз, которые можно разделить на три категории:

1) Угрозы безопасности, идущие от хоста — этот класс угроз включает: угрозы связи между виртуальной машиной (ВМ) и хостом, мониторинг виртуальной машины, изменения виртуальной машины;

2) Размещение вредоносного образа ВМ на физической системе: включает угрозы безопасности, происходящие от атак на пользователей и датацентры, потери и утечку информации, вредоносное воздействие и т.д.

3) Небезопасный программный интерфейс: включает угрозы, происходящие от особенностей ВМ.

В данном примере будем учитывать четырнадцать угроз и случай, когда нет угрозы.

Все права принадлежат издательству © NOTA BENE (ООО «НБ-Медиа») www.nbpublish.com

DOI: 10.7256/2073-8560.2013.6.9585

Нам необходимо знать вероятность возникновения каждой угрозы в час. Также необходимо указать значения вектора угроз, полученные в результате изучения системы.

Используя полученные матрицы и вектор угроз (таблица 4) можно посчитать стоимость потерь, вызванных ошибкой для каждой из сторон (таблица 5).

Потери для сторонявляются достаточно большими. Для того чтобы их сократить необходимо выявить уязвимости системы. Соотносим их с внешними и внутренними угрозами, ипринимаем необходимые контрмеры.

Подобное уточнение позволяет принять более обоснованные контрмеры. В данном случае — добавить межсетевой экран, прокси- и антивирусный сервер.

Заключение

В данной работе была рассмотрена модель анализа рисков ИБ и возможность ее использования для случая ОВ. Хотя требуется дальнейшее уточнение составляющих частей модели, даже в таком виде возможно ее успешное применение. Приведен пример использования данной модели, дающей правомерные оценки рисков, и подтверждающий, что она может быть применена для принятия решений.

Библиография

1. Zhang Jian Xun, Gu Zhi Min. Surey of research progress on cloud computing.Application Research of Computers, 2010, 27 (2).— PP. 429–433.
2. FENG Deng Guo, ZHANG Min, ZHANGYan, XUZhen.Study on Cloud Computing Security. Journal of Software, 2011, 22 (1).— PP. 71–83.
3. Michael Armbrust, Armando Fox, ReanGriffith.Above The Clouds: A Berkeley View of Cloud Computing. 2009, 2. EECS Department University of California, Berkeley Technical Report No. UCB /EECS 200928.http: //www.eecs. erkeley.edu /Pubs /TechRpts/2009/EECS-2009–28.pdf.
4. Царегородцев А. В., Качко А. К. Обеспечение информационной безопасности на облачной архитектуре организации // Национальная безопасность.— М.: Изд-во «НБ Медиа», 2011.—№ 5.— С. 25–34.
5. Царегородцев А. В., Качко А. К. Один из подходов к управлению информационной безопасностью при разработке информационной инфраструктуры организации // Национальная безопасность.— М.: Изд-во «НБ Медиа», 2012.—№ 1 (18).— С. 46–59.
6. Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, Joint Task Force Transformation Initiative, NIST Special Publication 800–37, Revision 1,.
7. Steve Elky. An Introduction to Information System Risk Management-SANS Institute, 2007.

References (transliterated)

1. Zhang Jian Xun, Gu Zhi Min. Surey of research progress on cloud computing.Application Research of Computers, 2010, 27 (2).— PP. 429–433.
2. FENG Deng Guo, ZHANG Min, ZHANGYan, XUZhen.Study on Cloud Computing Security. Journal of Software, 2011, 22 (1).— PP. 71–83.
3. Michael Armbrust, Armando Fox, ReanGriffith.Above The Clouds: A Berkeley View of Cloud

Все права принадлежат издательству © NOTA BENE (ООО «НБ-Медиа») www.nbpublish.com

DOI: 10.7256/2073-8560.2013.6.9585

Computing. 2009, 2. EECS Department University of California, Berkeley Technical Report No. UCB /EECS 200928.http: //www.eecs. erkeley.edu /Pubs /TechRpts/2009/EECS-2009–28.pdf.
4. Tsaregorodtsev A. V., Kachko A. K. Obespechenie informatsionnoi bezopasnosti na oblachnoi arkhitekture organizatsii // Natsional'naya bezopasnost».— M.: Izd-vo «NB Media», 2011.— № 5.— S. 25–34.
5. Tsaregorodtsev A. V., Kachko A. K. Odin iz podkhodov k upravleniyu informatsionnoi bezopasnost'yu pri razrabotke informatsionnoi infrastruktury organizatsii // Natsional'naya bezopasnost».— M.: Izd-vo «NB Media», 2012.—№ 1 (18).— S. 46–59.
6. Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, Joint Task Force Transformation Initiative, NIST Special Publication 800–37, Revision 1,.
7. Steve Elky. An Introduction to Information System Risk Management-SANS Institute, 2007.

Все права принадлежат издательству © NOTA BENE (ООО «НБ-Медиа») www.nbpublish.com

Статьи принимаются через сайт издательства www.nbpublish.com

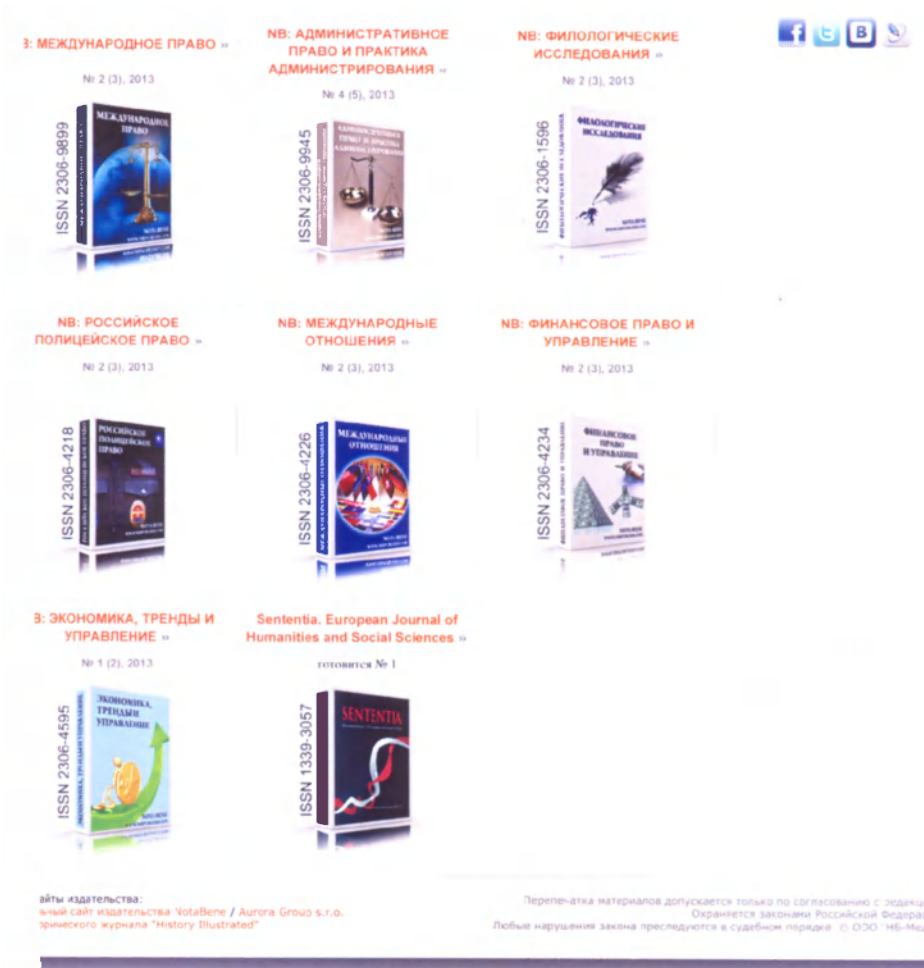
После регистрации на сайте следует прикрепить файл с аннотацией на русском языке в пять-шесть предложений, десять ключевых слов, раскрывающих смысл статьи, саму статью со сносками и список литературы по теме (библиографию) в десять-пятнадцать наименований.

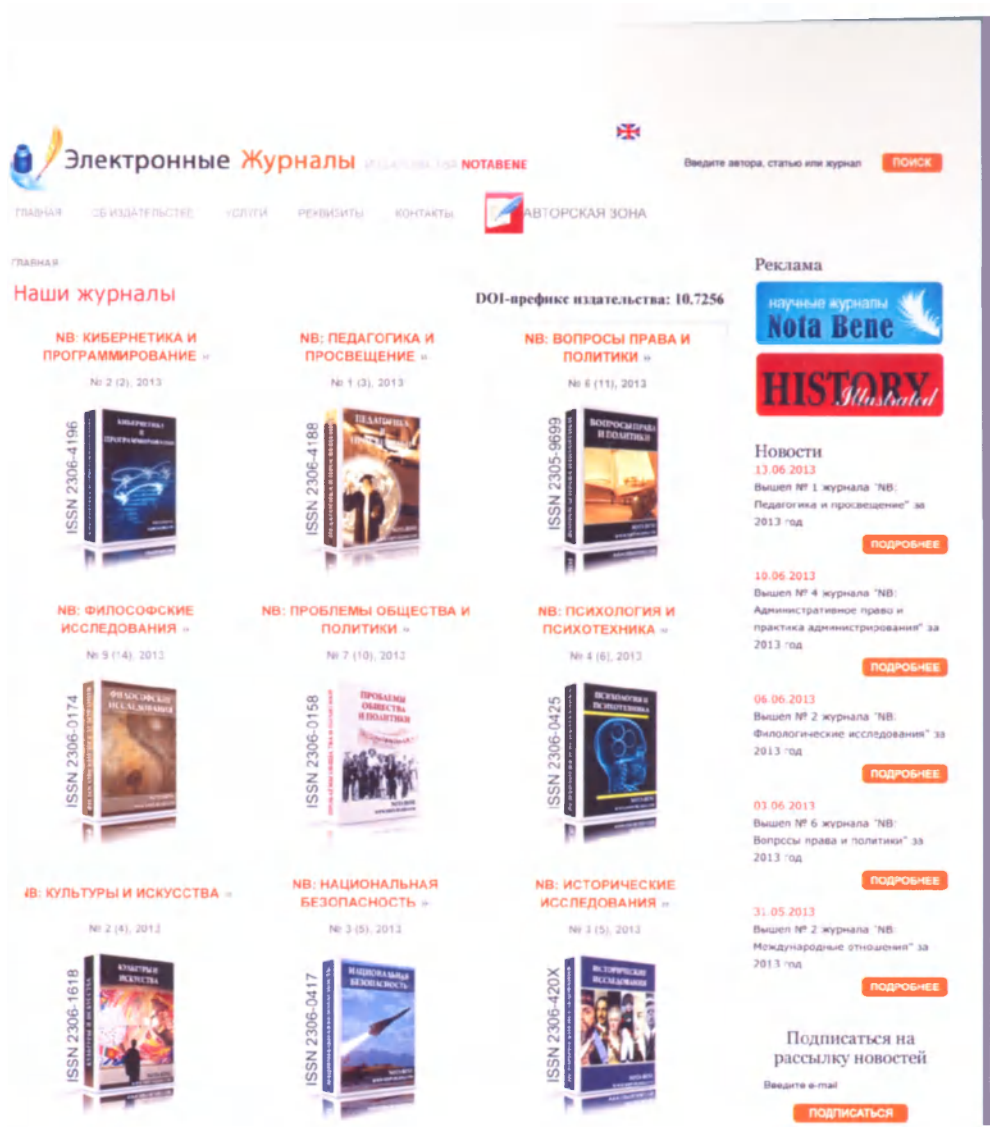
Журнал зарегистрирован Федеральной службой по надзору в сфере связи и массовых коммуникаций.
Свидетельство о регистрации: серия ПИ №ФС 77-35101 от 23 января 2009 г. Изд. лиц. № 065828 от 20.04.98 г.
Тел./факс: (495) 424-26-02 **Email:** w.danilenko@gmail.com
Внимание: отправка статей в редакцию возможна только через сайт издательства http://www.nbpublish.com
Почтовый адрес редакции: 117465, г. Москва, ул. Генерала Тюленева, 31/1-210.
ISSN 2073-8560
Объем 12,5 усл.-печ.л., формат 60x84 1/8. Тираж 1115 экз. Печать офсетная. Бумага офсетная.
Сдано в набор 30.12.2013. Подписано в печать 30.12.2013.
Отпечатано с PDF-файлов в Первой оперативной типографии
115114, г. Москва, Кожевнический пер.,12.
Подписка на журнал возможна с любого месяца.
Смотрите в Объединенном каталоге «ПРЕССА РОССИИ»
Наш индекс – 81935 (полугодовая и ежемесячнаяч подписка).
Любой журнал или статью можно заказать в магазине Книга-почтой
на сайте издательства www.nbpublish.com
Все права защищены и охраняются законодательством Российской Федерации об авторском праве. Ни одна из частей настоящего издания и весь журнал в целом не могут быть воспроизведены, переведены на другой язык, сохранены на печатных формах или любым другим способом обращены в иную форму хранения информации: электронным, механическим, фотокопировальным и другим – без предварительного согласования и письменного разрешения редакции. Ссылки на настоящее издание обязательны. За содержание опубликованной рекламы редакция ответственности не несет. Редакция сохраняет за собой право размещать материалы и статьи журнала в электронных правовых системах и иных электронных базах данных. Автор может известить редакцию о своем несогласии с подобным использованием его материалов не позднее даты подписания соответствующего номера в печать. Редакция уважает мнение авторов опубликованных статей, но при этом их мнение не всегда является мнением редакции журнала

Журнал **«Национальная безопасность»** включён в состав Перечня ведущих рецензируемых научных журналов и изданий, в которых должны быть опубликованы основные научные результаты диссертаций на соискание ученых степеней доктора и кандидата наук по специальностям: **экономика, военные и технические науки, политология, юриспруденция, социология, психология.** (Решение Президиума Высшей аттестационной комиссии Минобрнауки России от 19 февраля 2010 года №6/6)

Журнал включен в крупнейшую международную базу данных периодических изданий Ulrich's Periodicals Directory. Материалы журнала включены в систему Российского индекса научного цитирования.

© NOTA BENE (ООО «НБ-Медиа») www.nbpublish.com


3: МЕЖДУНАРОДНОЕ ПРАВО »
№ 2 (3), 2013
ISSN 2306-9899
NB: АДМИНИСТРАТИВНОЕ ПРАВО И ПРАКТИКА АДМИНИСТРИРОВАНИЯ »
№ 4 (5), 2013
ISSN 2306-9945
NB: ФИЛОЛОГИЧЕСКИЕ ИССЛЕДОВАНИЯ »
№ 2 (3), 2013
ISSN 2306-1596
NB: РОССИЙСКОЕ ПОЛИЦЕЙСКОЕ ПРАВО »
№ 2 (3), 2013
ISSN 2306-4218
NB: МЕЖДУНАРОДНЫЕ ОТНОШЕНИЯ »
№ 2 (3), 2013
ISSN 2306-4226
NB: ФИНАНСОВОЕ ПРАВО И УПРАВЛЕНИЕ »
№ 2 (3), 2013
ISSN 2306-4234
3: ЭКОНОМИКА, ТРЕНДЫ И УПРАВЛЕНИЕ »
№ 1 (2), 2013
ISSN 2306-4595
Sententia. European Journal of Humanities and Social Sciences »
готовится № 1
ISSN 1339-3057
SENTENTIA
айты издательства:
ный сайт издательства VotaBene / Aurora Group s.r.o.
рического журнала "History Illustrated"
Перепечатка материалов допускается только по согласованию с редакцией.
Охраняется законами Российской Федерации.
Любые нарушения закона преследуются в судебном порядке © ООО "Ив-Медиа"



Публикуйтесь
в электронных журналах.
Сетевые ресурсы эффективно
повышают Ваш рейтинг!

Журнал
"НАЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ/Nota bene"
решением Президиума Высшей аттестационной комиссии
Министерства образования и науки России
от 19 февраля 2010 г. №6/6
включен в новую редакцию
Перечня ведущих рецензируемых
научных журналов и изданий
в которых должны быть опубликованы
основные научные результаты
диссертаций на соискание ученых степеней
доктора и кандидата наук.

ВНИМАНИЮ АВТОРОВ:
все статьи принимаются
только через сайт издательства
www.nbpublish.com
вслед за регистрацией, необходимо
прикрепить аннотацию в 5-6 предложений
на русском языке,
десять ключевых слов
(словосочетания недопустимы),
статью с постраничными сносками,
список литературы в 10-15 наименований.

ISSN 2073856
9 772073 856000