"Доктрина информационной безопасности Российской Федерации" — опыт количественного моделирования

В. М. Шишкин, Р. М. Юсупов
Санкт-Петербургский институт информатики и автоматизации РАН
199178, Санкт-Петербург, 14-я линия В.О., д.39
spiiran@iias.spb.su

УДК 519.6
В. М. Шишкин, Р. М. Юсупов. **"Доктрина информационной безопасности Российской Федерации" — опыт количественного моделирования** // Труды СПИИРАН. Вып. 1, т. 1. - СПб: СПИИРАН, 2002.

Аннотация. *Дается формализованное представление "Доктрины информационной безопасности" в терминах и средствами модели, разработанной для анализа и оценивания защищенности информационных объектов. Подчеркивается совпадение основных категорий, используемых, как в модели, так и в "Доктрине", что позволило провести естественную формализацию содержания данного документа. Приводятся результаты оценочных расчетов, в том числе, дается количественная оценка мер, предлагаемых в "Доктрине" и иных, подобного масштаба, документах. Показывается возможность применения модели для поддержки реализации "Доктрины" на инженерном уровне и для ее собственного развития.* — Библ. 4 назв.

UDC 519.6
V. M. Shishkin, R. M. Yusupov. **"The Doctrine of information security of Russian Federation" — an experience of quantitative modeling** // SPIIRAS Proceedings. Issue 1, v. 1. - SPb: SPIIRAS, 2002.

Abstract. *Formalized presentation of "The Doctrine of information security" is given in term and facility of the model designed for analysis and security estimation of information objects. It is emphasized coincidence of main categories, used, both in model, and in "The Doctrine" that has allowed to conduct the natural formalization of the contents given document. It is brought results of merit calculation including quantitative estimation of the measures, proposed in "Doctrine" and the other documents like level. It is shown possibility of the using of model for support of the realization of "The Doctrine" on engineering level and for her own development.* — Bibl. 4 items.

1. Введение

Концептуальные и научно-методологические основы информационной безопасности еще только начинают разрабатываться. Поэтому научно обоснованная структуризация проблемы, терминология и многие другие ее аспекты должны быть предметами дальнейших разработок. В СПИИРАН, являющимся головной организацией по научно-методологическому сопровождению информатизации города, исследования и разработки по проблемам информационной безопасности, в том числе в общесистемном контексте проблем информатизации, ведутся уже на протяжении ряда лет [1]. Существенным событием для исследования указанных проблем является утверждение Президентом РФ "Доктрины информационной безопасности Российской Федерации" [2]. Являясь прежде всего политическим документом, допускающим декларативный характер, она, тем не менее, представляется одним из немногих примеров близкого к системному целостного представления проблемы информационной безопасности, дает основу для ее отображения в хорошо структурированном виде, допускающим формализацию. Последнее обстоятельство весьма существенно, так как появляется возможность моделирования ситуаций, объективизации исследований и принятия количественно обоснованных целенаправленных решений не спекулятивного характера, то есть политический документ может стать основой для

Труды СПИИРАН. 2002. Вып. 1. Т. 1. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2002. Issue 1. V. 1. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

исследований и рекомендаций на инженерном уровне. Настоящая работа является перспективным примером такого исследования.

2. Спецификация модели "Доктрины"

Формально содержание "Доктрины", во всяком случае, первого ее раздела, можно свести к следующим основным классам представлений, сгруппированных в табличном виде (для упрощения и в силу некоторых пересечений содержания разделов в "Доктрине" использовался именно первый ее раздел):

1) источники угроз информационной безопасности РФ (табл. 1);
2) угрозы информационной безопасности РФ (табл. 2);
3) объект защиты — "национальные интересы Российской Федерации в информационной сфере", задаваемый набором компонентов, называемых "Составляющие национальных интересов Российской Федерации в информационной сфере" (табл. 3) или, на более детальном уровне, "объектами обеспечения информационной безопасности Российской Федерации" (здесь не рассматриваются);
4) меры по обеспечению защищенности национальных интересов РФ в информационной сфере (табл. 4).

Индексация элементов в таблицах внутренняя (#) и сквозная (№), содержание соответствует тексту оригинала.

Как оказалось, приведенные классы понятий "Доктрины", практически эквивалентны множествам элементов модели [3], ранее разработанной для анализа безопасности информационных объектов. Представления модели, в силу ее технической направленности, имеют более узкий, но не противоречащий понятиям "Доктрины", смысл. Это обстоятельство позволило применить ее методический и алгоритмический аппарат, соответствующие программные средства для формализованного анализа "Доктрины" и получения некоторых полезных количественных оценок.

В кратком изложении, использованная модель основана на дихотомической оппозиции: "защищаемый объект", с одной стороны, и, с другой, - считающаяся потенциально враждебной "среда". Выделяются три непересекающихся подмножества множества элементов модели: "источники угроз", досягаемостью которых определяется внешняя граница среды; "угрозы безопасности", порождаемые источниками; "компоненты объекта", на которые воздействуют реализованные угрозы. Источники угроз определяются как "субъекты воздействий", все остальные факторы воздействий на защищаемый объект квалифицируются в качестве угроз, реализации которых определяются как "события", а компоненты - как объекты воздействий.

Считается, что на множестве элементов модели может быть определено бинарное отношение "быть причиной" со свойством транзитивности, фиксирующее каналы распространения потоков угроз. Таким образом, защищаемый объект подвергается воздействию генерируемого источниками совокупного потока реализованных угроз, взвешенного соответственно их значимости. Эти воздействия влияют на его "состояние защищенности", характеризуемое измеримыми показателями. В исходном состоянии их значения принимаются равными 1.

Таким образом, основная и наиболее ответственная с точки зрения доверия к получаемым результатам задача конкретного анализа состоит в установлении непосредственных причинно-следственных отношений между всеми элементами модели, то есть задание ее причинной структуры, представляемой в виде матрицы бинарных отношений **W**. Структура

Труды СПИИРАН. 2002. Вып. 1. Т. 1. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2002. Issue 1. V. 1. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

определяется пока экспертным путем, но ведутся разработки по автоматизации процесса ее построения с использованием базы знаний. Далее, ненулевые элементы матрицы **W** тем или иным образом получают метрические оценки, в конечном итоге имеющие смысл нормированных по столбцам весовых коэффициентов w_{ij}. На рис. 1 представлена данная матрица в блочном виде, на которой хорошо видна структура модели, в том числе ограничения в виде нулевых блоков.

Таблица 1. Источники угроз национальным интересам РФ в информационной сфере.

№	#	Содержание элемента
1	1	Деятельность иностранных политических, экономических, военных, разведывательных и информационных структур, направленная против интересов Российской Федерации в информационной сфере.
2	2	Стремление ряда стран к доминированию и ущемлению интересов России в мировом информационном пространстве, вытеснению ее с внешнего и внутреннего информационных рынков.
3	3	Обострение международной конкуренции за обладание информационными технологиями и ресурсами.
4	4	Деятельность международных террористических организаций.
5	5	Увеличение технологического отрыва ведущих держав мира, наращивание их возможностей по противодействию созданию конкурентоспособных российских информационных технологий.
6	6	Деятельность космических, воздушных, морских и наземных технических и иных средств (видов) разведки иностранных государств.
7	7	Разработка рядом государств концепций информационных войн, предусматривающих создание средств опасного воздействия на информационные сферы других стран мира, нарушение нормального функционирования информационных и телекоммуникационных систем, сохранности информационных ресурсов, получение несанкционированного доступа к ним.
8	8	Критическое состояние отечественных отраслей промышленности.
9	9	Неблагоприятная криминогенная обстановка, сопровождающаяся тенденциями сращивания государственных и криминальных структур в информационной сфере, получения криминальными структурами доступа к конфиденциальной информации, усиления влияния организованной преступности на жизнь общества, снижения степени защищенности законных интересов граждан, общества и государства в информационной сфере.
10	10	Недостаточная координация деятельности федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации по формированию и реализации единой государственной политики в области обеспечения информационной безопасности Российской Федерации.
11	11	Недостаточная разработанность нормативной правовой базы, регулирующей отношения в информационной сфере, а также недостаточная правоприменительная практика.
12	12	Неразвитость институтов гражданского общества и недостаточный государственный контроль за развитием информационного рынка России.
13	13	Недостаточное финансирование мероприятий по обеспечению информационной безопасности Российской Федерации.
14	14	Недостаточная экономическая мощь государства.
15	15	Снижение эффективности системы образования и воспитания, недостаточное количество квалифицированных кадров в области обеспечения информационной безопасности.
16	16	Недостаточная активность федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации в информировании общества о своей деятельности, в разъяснении принимаемых решений, в формировании открытых государственных ресурсов и развитии системы доступа к ним граждан.

Труды СПИИРАН. 2002. Вып. 1. Т. 1. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2002. Issue 1. V. 1. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

17	17	Отставание России от ведущих стран мира по уровню информатизации федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и органов местного самоуправления, кредитно-финансовой сферы, промышленности, сельского хозяйства, образования, здравоохранения, сферы услуг и быта граждан.

Таблица 2. Угрозы национальным интересам РФ в информационной сфере.

№	#	Содержание элемента
18	1	Принятие федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации нормативных правовых актов, ущемляющих конституционные права и свободы граждан в области духовной жизни и информационной деятельности.
19	2	Создание монополий на формирование, получение и распространение информации в Российской Федерации, в том числе с использованием телекоммуникационных систем.
20	3	Противодействие, в том числе со стороны криминальных структур, реализации гражданами своих конституционных прав на личную и семейную тайну, тайну переписки, телефонных переговоров и иных сообщений.
21	4	Нерациональное, чрезмерное ограничение доступа к общественно необходимой информации.
22	5	Противоправное применение специальных средств воздействия на индивидуальное, групповое и общественное сознание.
23	6	Неисполнение федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, органами местного самоуправления, организациями и гражданами требований федерального законодательства, регулирующего отношения в информационной сфере.
24	7	Неправомерное ограничение доступа граждан к открытым информационным ресурсам федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления, к открытым архивным материалам, к другой открытой социально значимой информации.
25	8	Дезорганизация и разрушение системы накопления и сохранения культурных ценностей, включая архивы.
26	9	Нарушение конституционных прав и свобод человека и гражданина в области массовой информации.
27	10	Вытеснение российских информационных агентств, средств массовой информации с внутреннего информационного рынка и усиление зависимости духовной, экономической и политической сфер общественной жизни России от зарубежных информационных структур.
28	11	Девальвация духовных ценностей, пропаганда образцов массовой культуры, основанных на культе насилия, на духовных и нравственных ценностях, противоречащих ценностям, принятым в российском обществе.
29	12	Снижение духовного, нравственного и творческого потенциала населения России, что существенно осложнит подготовку трудовых ресурсов для внедрения и использования новейших технологий, в том числе информационных.
30	13	Манипулирование информацией (дезинформация, сокрытие или искажение информации).
31	14	Монополизация информационного рынка России, его отдельных секторов отечественными и зарубежными информационными структурами.
32	15	Блокирование деятельности государственных средств массовой информации по информированию российской и зарубежной аудитории.
33	16	Низкая эффективность информационного обеспечения государственной политики Российской Федерации вследствие дефицита квалифицированных кадров, отсутствия системы формирования и реализации государственной информационной политики.

Труды СПИИРАН. 2002. Вып. 1. Т. 1. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2002. Issue 1. V. 1. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

34	17	Противодействие доступу Российской Федерации к новейшим информационным технологиям, взаимовыгодному и равноправному участию российских производителей в мировом разделении труда в индустрии информационных услуг, средств информатизации, телекоммуникации и связи, информационных продуктов, а также создание условий для усиления технологической зависимости России в области современных информационных технологий.
35	18	Закупка органами государственной власти импортных средств информатизации, телекоммуникации и связи при наличии отечественных аналогов, не уступающих по своим характеристикам зарубежным образцам.
36	19	Вытеснение с отечественного рынка российских производителей средств информатизации, телекоммуникации и связи.
37	20	Увеличение оттока за рубеж специалистов и правообладателей интеллектуальной собственности.
38	21	Противоправные сбор и использование информации.
39	22	Нарушения технологии обработки информации.
40	23	Внедрение в аппаратные и программные изделия компонентов, реализующих функции, не предусмотренные документацией на эти изделия.
41	24	Разработка и распространение программ, нарушающих нормальное функционирование информационных и информационно-телекоммуникационных систем, в том числе систем защиты информации.
42	25	Уничтожение, повреждение, радиоэлектронное подавление или разрушение средств и систем обработки информации, телекоммуникации и связи.
43	26	Воздействие на парольно-ключевые системы защиты автоматизированных систем обработки и передачи информации.
44	27	Компрометация ключей и средств криптографической защиты информации.
45	28	Утечка информации по техническим каналам.
46	29	Внедрение электронных устройств для перехвата информации в технические средства обработки, хранения и передачи информации по каналам связи, а также в служебные помещения органов государственной власти, предприятий, учреждений и организаций независимо от формы собственности.
47	30	Уничтожение, повреждение, разрушение или хищение машинных и других носителей информации.
48	31	Перехват информации в сетях передачи данных и на линиях связи, дешифрование этой информации и навязывание ложной информации.
49	32	Использование несертифицированных отечественных и зарубежных информационных технологий, средств защиты информации, средств информатизации, телекоммуникации и связи при создании и развитии российской информационной инфраструктуры.
50	33	Несанкционированный доступ к информации, находящейся в банках и базах данных.
51	34	Нарушение законных ограничений на распространение информации.

Таблица 3. Составляющие (компоненты) национальных интересов РФ в информационной сфере.

№	#	Содержание элемента
5 2	**I**	Соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею, обеспечение духовного обновления России, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны.
5 3	**II**	Информационное обеспечение государственной политики Российской Федерации, связанное с доведением до российской и международной общественности достоверной информации о государственной политике Российской Федерации, ее официальной позиции по социально значимым событиям российской и международной жизни, с обеспечением доступа граждан к открытым государственным информационным ресурсам.

Труды СПИИРАН. 2002. Вып. 1. Т. 1. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2002. Issue 1. V. 1. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

54	**III**	Развитие современных информационных технологий, отечественной индустрии информации, в том числе индустрии средств информатизации, телекоммуникации и связи, обеспечение потребностей внутреннего рынка ее продукцией и выход этой продукции на мировой рынок, а также обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов.
55	**IV**	Защита информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем, как уже развернутых, так и создаваемых на территории России.

Таблица 4. Требуемые меры по обеспечению защищенности национальных интересов РФ в информационной сфере.

#	**Содержание мер**
1	Повысить эффективность использования информационной инфраструктуры в интересах общественного развития, консолидации российского общества, духовного возрождения многонационального народа Российской Федерации.
2	Усовершенствовать систему формирования, сохранения и рационального использования информационных ресурсов, составляющих основу научно-технического и духовного потенциала Российской Федерации.
3	Обеспечить конституционные права и свободы человека и гражданина свободно искать, получать, передавать, производить и распространять информацию любым законным способом, получать достоверную информацию о состоянии окружающей среды.
4	Обеспечить конституционные права и свободы человека и гражданина на личную и семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, на защиту своей чести и своего доброго имени.
5	Укрепить механизмы правового регулирования отношений в области охраны интеллектуальной собственности, создать условия для соблюдения установленных федеральным законодательством ограничений на доступ к конфиденциальной информации.
6	Гарантировать свободу массовой информации и запрет цензуры.
7	Не допускать пропаганду и агитацию, которые способствуют разжиганию социальной, расовой, национальной или религиозной ненависти и вражды.
8	Обеспечить запрет на сбор, хранение, использование и распространение информации о частной жизни лица без его согласия и другой информации, доступ к которой ограничен федеральным законодательством.
9	Укреплять государственные средства массовой информации, расширять их возможности по своевременному доведению достоверной информации до российских и иностранных граждан.
10	Интенсифицировать формирование открытых государственных информационных ресурсов, повысить эффективность их хозяйственного использования.
11	Развивать и совершенствовать инфраструктуру единого информационного пространства Российской Федерации.
12	Развивать отечественную индустрию информационных услуг и повышать эффективность использования государственных информационных ресурсов.
13	Развивать производство в Российской Федерации конкурентоспособных средств и систем информатизации, телекоммуникации и связи, расширять участие России в международной кооперации производителей этих средств и систем.
14	Обеспечить государственную поддержку отечественных фундаментальных и прикладных исследований, разработок в сферах информатизации, телекоммуникации и связи.

Труды СПИИРАН. 2002. Вып. 1. Т. 1. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2002. Issue 1. V. 1. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

15	Повысить безопасность информационных систем, включая сети связи, прежде всего безопасность первичных сетей связи и информационных систем федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, финансово-кредитной и банковской сфер, сферы хозяйственной деятельности, а также систем и средств информатизации вооружения и военной техники, систем управления войсками и оружием, экологически опасными и экономически важными производствами.
16	Интенсифицировать развитие отечественного производства аппаратных и программных средств защиты информации и методов контроля за их эффективностью.
17	Обеспечить защиту сведений, составляющих государственную тайну.
18	Расширять международное сотрудничество Российской Федерации в области развития и безопасного использования информационных ресурсов, противодействия угрозе развязывания противоборства в информационной сфере.

W		1	2	3	4
1	Источники угроз	**0**	$W_{иу}$	**0**	**0**
2	Угрозы	**0**	$W_{уу}$	$W_{ук}$	**0**
3	Объект (компоненты)	**0**	$W_{ку}$	**0**	W_{kz}
4	Состояние объекта	**0**	**0**	**0**	**0**

V		1	2	3	4
1	Источники угроз	**0**	$V_{иу}$	$V_{ик}$	$V_{иz}$
2	Угрозы	**0**	$V_{уу}$	$V_{ук}$	$V_{уz}$
3	Объект (компоненты)	**0**	$V_{ку}$	$V_{кк}$	V_{kz}
4	Состояние объекта	**0**	**0**	**0**	**0**

Рисунок 1. Схема модели в матричном виде (полная матрица отношений)

Первая расчетная задача, решаемая на матрице **W**, состоит в получении оценок отношений между элементами модели, но, в отличие от **W**, уже с учетом их транзитивности (матрица **V**), которые для сложных структур даже на качественном уровне далеко не очевидны, и, тем более, трудно дать им обоснованную количественную оценку. Блочная структура **V** приведена также на рис. 1. Блоки, содержащиеся в 4-ом столбце **V** вырожденные и представляют собой вектор наиболее существенных оценок — показателей влияния всех выделенных в модели факторов на состояние защищенности объекта, которые являются основой для дальнейшего анализа и, возможно, синтеза и оценивания мер противодействия.

В случае приводимой к треугольному виду матрицы **W** значение каждого элемента v_{ij} из **V** легко определить известным образом в терминах инвариантного матричному графического представления, как сумму по всем путям из i-ой вершины в j-ую произведений весов дуг по каждому пути. Однако в общем случае такой способ не приемлем, и задача решается с использованием аппарата Марковских цепей: $\mathbf{V}=(\mathbf{I}-\mathbf{W})^{-1}-\mathbf{I}$, где $\mathbf{I}$ — единичная матрица (в используемом программном средстве применен более эффективный и устойчивый алгоритм).

Любая система мер и средств имеет цель изменения исходного состояния защищаемого объекта в ту или иную сторону и всегда решает задачу модификации конечного потока угроз. Осуществляется это в результате локальных воздействий на включенные в модель факторы возникновения и распространения угроз, что количественно характеризуется параметрами, имеющими смысл усиливающих или понижающих коэффициентов, $r_i \leq 1$.

Интегральная результативность системы воздействий в целом на объект характеризуется имеющим тот же смысл вычисляемым показателем $r_z<1$, определяющим относительное изменение состояния защищенности. Формально r_z может равняться 1, но практически это недостижимо, поэтому для него определяется строгое неравенство. Тогда, инвариантно новое состояние, в частности, характеризуется также относительным показателем уровня защищенности $s_z=(1-r_z)^{-1}>0$. Отрицательные значения r_z и, соответственно, $s_z<1$

Труды СПИИРАН. 2002. Вып. 1. Т. 1. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2002. Issue 1. V. 1. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

будут свидетельствовать о снижении уровня защищенности объекта. Допускается противоречивая направленность воздействий.

Если не принимать во внимание оценочный аспект, то очевидно, даже на уровне терминологии, совпадение абстрактных представлений модели и конкретных положений "Доктрины". Отличие состоит в том, что в "Доктрине" не определяются отношения между элементами, хотя именно взаимодействие различных факторов, влияющих на безопасность, имеет существенное значение для оценки их конечной значимости и, соответственно, для определения наиболее целесообразных и эффективных мер и средств повышения уровня безопасности. Не предполагается "Доктриной" и получение каких-либо количественных оценок. Тем не менее, документ дает основу для конструктивного решения этих задач, и в первом приближении, в качестве опыта, такая работа проделана.

Проведена структуризация элементов "Доктрины", ее результаты в соответствии с алгоритмическими требованиями модели представлены блоками матрицы отношений **W**: ($\mathbf{W}_{ИУ}$ — источники угроз-угрозы) — рис. 2, ($\mathbf{W}_{УУ}$ — угрозы-угрозы) — рис. 3, ($\mathbf{W}_{УК}$ — угрозы-компоненты) — рис. 4, (меры-факторы) — рис. 5. На рис. 4 для удобства матрица представлена в транспонированном виде. $\mathbf{W}_{КУ}$ - в нашем случае нулевая, а $\mathbf{W}_{УК}$ — тривиальна.

Весовые коэффициенты w_{ij} в матрицах на рис. 2–4 определялись, исходя из двух вариантов ситуаций:

1) отсутствие априорной информации о соотношении значимости различных факторов (в этом случае предполагалась их равновесность, то есть равенство w_{ij} по столбцам);
2) наличие некоторой информации, позволяющей провести ординальное оценивание, то есть установление отношения порядка между факторами, с последующей арифметизацией значений.

Существенного, качественного различия результатов расчетов по ним не наблюдалось. Поэтому ниже для иллюстрации представлен количественный анализ, проведенный по первому варианту, поскольку в этом случае, прежде всего, проявляются структурные свойства модели, более определенные в отличие от индивидуальных весовых коэффициентов w_{ij}.

		Угрозы																																				
		I													II		III				IV																	
		18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51
Источники угроз	внутренние	1	0	0,072	0,112	0	0,084	0,112	0	0,125	0	0,076	0,084	0,076	0,047	0,072	0,066	0	0,1	0,112	0,076	0,076	0,044	0	0,084	0,076	0,09	0,084	0,062	0,084	0,076	0,066	0,072	0	0,058	0,062
		2	0	0,072	0	0	0	0	0	0	0	0,077	0,084	0,077	0,047	0,072	0,066	0	0,1	0	0,077	0,077	0,044	0	0	0,077	0	0	0	0	0	0	0	0	0,058	0,062
		3	0	0,072	0	0	0	0	0	0	0	0,077	0	0	0	0,072	0	0	0,1	0	0,077	0,077	0,044	0	0	0	0	0	0	0	0	0,066	0,072	0	0,058	0,062
		4	0	0	0,111	0	0,084	0	0	0	0	0	0	0	0,047	0	0,066	0	0	0	0	0	0,044	0	0,084	0,077	0,091	0,084	0,062	0,084	0,077	0,066	0,072	0	0,059	0
		5	0	0,072	0	0	0	0	0	0	0	0,077	0	0	0	0,072	0	0,1	0	0,111	0,077	0,077	0	0,112	0	0	0	0	0	0	0,077	0	0	0,09	0	0
		6	0	0	0,111	0	0,084	0	0	0	0	0	0	0	0,047	0	0,066	0	0	0	0	0	0,044	0	0	0	0,091	0,084	0,062	0,084	0	0	0,072	0	0,059	0,062
		7	0	0	0	0	0,084	0	0	0,125	0	0,077	0,084	0,077	0,047	0,072	0,066	0	0,1	0	0	0,077	0,044	0	0,084	0,077	0,091	0,084	0,062	0,084	0,077	0,066	0,072	0	0,059	0,062
	внешние	8	0	0,072	0	0	0	0	0	0	0	0	0	0	0	0,072	0	0,1	0,1	0,111	0,077	0,077	0	0,111	0,084	0,077	0	0	0	0	0,077	0	0	0,091	0	0
		9	0,166	0,072	0,111	0,072	0,083	0,111	0,072	0	0,062	0	0	0	0,047	0	0,067	0	0	0	0	0	0,044	0	0,083	0,077	0,091	0,083	0,062	0,083	0,077	0,066	0,072	0	0,059	0,062
		10	0,166	0,071	0	0,072	0	0,111	0,072	0,125	0,062	0,077	0,084	0	0	0,071	0	0,1	0	0,111	0,077	0,077	0,044	0,111	0,083	0,077	0	0	0	0	0,077	0	0	0,091	0	0,062
		11	0,167	0,071	0,111	0,072	0,083	0,111	0,072	0,125	0,062	0,077	0,083	0,077	0,047	0,071	0	0,1	0	0,111	0,077	0,077	0,044	0	0	0	0	0	0	0	0	0	0	0,091	0,059	0,062
		12	0,167	0,071	0,111	0,072	0	0,111	0,072	0,125	0,062	0	0,083	0	0,047	0,071	0,067	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,063
		13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,111	0	0	0	0	0	0,083	0,077	0,067	0	0,091	0	0
		14	0	0,071	0	0	0	0	0	0,125	0	0,077	0	0,077	0	0,071	0	0,1	0,1	0	0,077	0,077	0	0	0,083	0,077	0	0	0	0	0	0	0	0,091	0	0
		15	0	0	0	0	0	0	0	0	0	0,083	0,077	0,048	0	0	0,1	0,1	0	0,077	0,077	0,044	0,111	0	0	0	0	0	0	0,077	0	0	0,091	0,059	0
		16	0	0	0	0,072	0	0,111	0,072	0	0,062	0	0	0	0,048	0	0,067	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,063
		17	0	0,071	0,111	0,072	0	0	0,072	0	0,062	0,077	0	0	0,048	0,071	0,067	0,1	0,1	0,111	0,077	0,077	0	0,111	0,083	0,077	0	0	0	0	0,077	0	0	0,091	0	0

Рисунок 2. Матрица отношений "источники угроз - угрозы" ($\mathbf{W}_{ИУ}$)

3. Результаты анализа модели

Таким образом, была определена и оценена полная матрица отношений, что явилось достаточным для проведения комплекса аналитических расчетов

Труды СПИИРАН. 2002. Вып. 1. Т. 1. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2002. Issue 1. V. 1. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

на модели. Во-первых, были получены значения оценок транзитивных отношений, учитывающих сложные, опосредованные связи между элементами, и, в том числе, значения показателей влияния всех элементов на состояние защищенности объекта — "национальных интересов РФ в информационной сфере", то есть, рассчитана матрица **V** и ее последний вектор-стобец $\mathbf{v}_Z$. Для равновесного варианта расчетов оценки представлены на рис. 6 в порядке убывания их значимости отдельно для источников угроз и угроз. Как видно из диаграммы, в обоих множествах можно выделить группы наиболее значимых факторов.

		Угрозы																																	
		I													II			III				IV													
		18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51
Угрозы I	18		0,071	0	0,071	0	0	0	0	0,062	0,077	0	0	0	0,071	0	0	0	0	0	0	0,044	0	0	0	0	0	0	0	0	0	0	0	0	0
	19	0		0	0,071	0,083	0	0,071	0	0,062	0,077	0,083	0	0,048	0,071	0,067	0	0	0	0,077	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	20	0,167	0		0,071	0	0,111	0,071	0	0,063	0	0	0	0	0	0,067	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	21	0	0	0		0	0	0	0	0,063	0	0	0	0,048	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	22	0	0	0	0		0	0	0	0,063	0	0,083	0,077	0,048	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	23	0	0,071	0	0,071	0,083		0,071	0,125	0,063	0	0	0	0,048	0	0,067	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	24	0	0	0	0	0	0		0	0,063	0	0	0	0,048	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	25	0	0	0	0	0	0	0,071		0	0	0,083	0,077	0,048	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	26	0	0	0	0	0	0	0	0		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	27	0	0	0,111	0,071	0,083	0	0,071	0	0,063		0,083	0,077	0,048	0	0,067	0,1	0	0	0,077	0	0,043	0	0	0	0	0	0	0	0	0	0	0	0	0
	28	0	0	0	0	0	0	0	0	0	0		0,077	0	0	0	0	0	0	0	0,077	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	29	0	0	0	0	0	0	0	0	0	0	0		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	30	0	0	0	0	0	0	0	0	0,063	0	0	0,077		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
II	31	0	0	0,111	0,071	0,083	0	0,071	0	0,063	0,077	0,083	0,077	0,048		0,067	0	0,1	0,111	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,063
	32	0	0	0	0,071	0,083	0	0,071	0	0	0	0	0	0,048	0		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	33	0,167	0	0	0	0	0,111	0,071	0	0	0	0	0	0	0	0,067		0	0	0	0	0	0,111	0	0	0	0	0,062	0	0	0	0	0	0	0
III	34	0	0,071	0	0,071	0	0	0	0,125	0	0,077	0	0	0	0	0	0,1		0,111	0,077	0	0	0	0,083	0,077	0,091	0	0	0	0	0	0	0,091	0	0
	35	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0		0	0	0,043	0	0,083	0,077	0,091	0,083	0,062	0,083	0,077	0,067	0,071	0,091	0,059	0
	36	0	0	0	0	0,083	0,111	0	0	0	0	0	0	0,048	0,071	0	0	0	0,111		0,077	0,043	0	0,083	0,077	0	0	0,062	0	0,077	0	0	0,091	0	0
	37	0	0	0	0	0	0	0	0	0	0	0	0,077	0	0	0	0,1	0,1	0	0		0	0	0	0	0	0,083	0,063	0	0	0	0	0	0	0,063
IV	38	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0		0	0	0	0	0	0,063	0	0	0	0	0	0	0,063
	39	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,043		0	0	0,091	0,083	0,063	0,083	0	0,067	0,071	0	0,059	0
	40	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,043	0,111		0	0,091	0,083	0,063	0,083	0	0,067	0,071	0	0,059	0
	41	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,043	0,111	0		0,091	0,083	0,063	0,083	0	0,067	0,071	0	0,059	0
	42	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,043	0	0	0		0	0	0	0	0,067	0	0	0	0
	43	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,043	0	0	0	0		0	0	0	0,067	0,071	0	0,059	0
	44	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,083		0	0	0,067	0,071	0	0,059	0
	45	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,043	0	0	0	0	0	0,063		0	0	0	0	0	0,063
	46	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,063	0		0	0,071	0	0,059	0
	47	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0		0	0	0	0
	48	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,043	0	0	0	0	0	0	0,083	0	0		0	0	0,063
	49	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,043	0	0,083	0,077	0,091	0,083	0,063	0,083	0,077	0,067	0,071		0,059	0
	50	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,043	0	0	0	0	0	0	0	0	0,067	0	0		0,063
	51	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	

Рисунок 3. Матрица отношений "угрозы - угрозы" ($\mathbf{W}_{yy}$)

		Угрозы																																	
		I													II			III				IV													
		18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51
Объект I	52	0,066	0,066	0,066	0,066	0,066	0,067	0,067	0,067	0,067	0,067	0,067	0,067	0,067	0,067	0,067	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
II	53	0	0,052	0	0	0	0,052	0	0,052	0	0,052	0	0	0,052	0,052	0,052	0,053	0	0,053	0	0	0	0,053	0,053	0,053	0,053	0	0	0	0,053	0,053	0,053	0,053	0,053	0,053
III	54	0	0,142	0	0	0	0	0	0	0	0,143	0	0	0	0,143	0	0	0,143	0,143	0,143	0,143	0	0	0	0	0	0	0	0	0	0	0	0	0	0
IV	55	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,055	0,055	0,055	0,055	0,055	0,055	0,055	0,055	0,056	0,056	0,056	0,056	0,056	0,056	0,056	0,056	0,056	0,056

Рисунок 4. Матрица отношений "угрозы - компоненты" ($\mathbf{w}_{yk}$)

Воздействия		Источники угроз: внешние							внутренние									
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
I	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
	2	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	1	1
	3	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1	0
	4	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0
	5	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0
	6	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0
	7	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0
	8	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0
II	9	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	10	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1
III	11	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1
	12	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1
	13	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1
	14	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0
IV	15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	17	1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0
	18	1	1	1	1	1	0	1	0	0	0	0	0	0	0	0	0	0

Воздействия		У г р о з ы: I													II			III				IV													
		18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51
I	1	0	0	0	1	0	1	1	1	1	1	1	0	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
	2	0	0	0	1	0	1	1	1	1	1	1	0	1	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	3	1	0	0	1	0	1	1	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	4	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1	1
	5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1	0
	6	1	1	0	1	0	0	1	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	7	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	8	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1	1
II	9	0	1	0	0	0	0	0	0	0	1	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	10	0	1	0	1	0	0	1	1	1	0	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
III	11	0	0	0	0	0	0	0	1	0	1	0	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	12	0	0	0	1	0	0	1	0	0	1	0	0	0	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0
IV	15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0	1	0	1	0
	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	1	1	0	0	0	1	0	0	1	0	0
	17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	0	1	0	0	1
	18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Рисунок 5. Матрица отношений "меры - факторы"

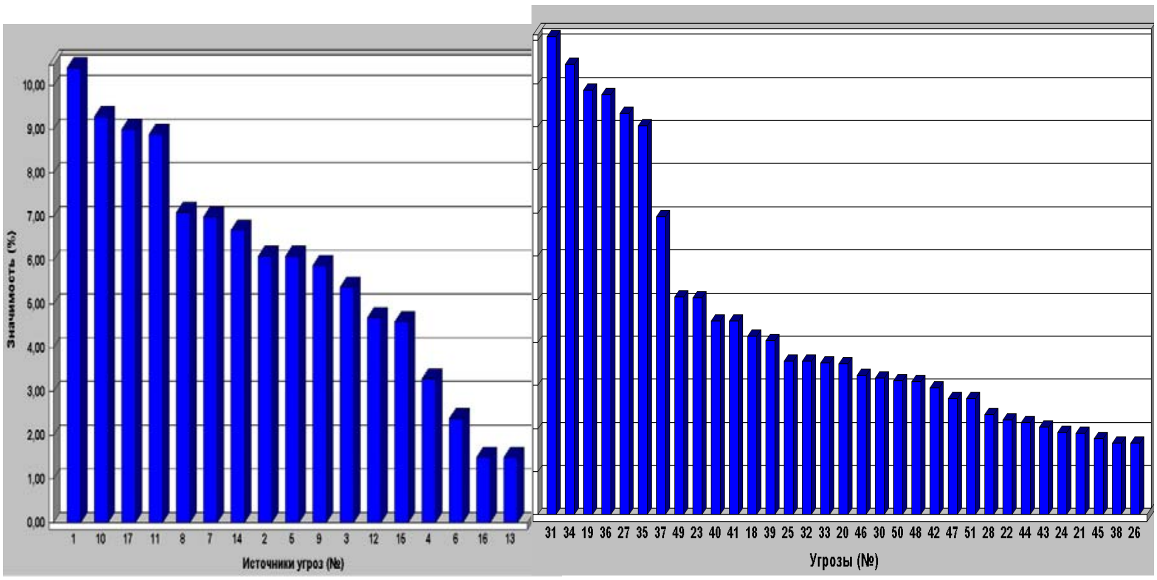

Рисунок 6. Диаграмма значимости факторов, угрожающих национальным интересам РФ в информационной сфере ($\mathbf{v}_z$)

Для источников угроз 4 их вида из 17 дали около 40% суммарного влияния на состояние защищенности:

- (1) "Деятельность иностранных политических, экономических, военных, разведывательных и информационных структур, направленная против интересов Российской Федерации в информационной сфере" — (10,4%);
- (10) "Отставание России от ведущих стран мира по уровню информатизации …" — (9,3%);
- (17) "Недостаточная координация деятельности … по формированию и реализации единой государственной политики в области обеспечения информационной безопасности Российской Федерации" — (9,0%);
- (11) "Недостаточная разработанность нормативной правовой базы, регулирующей отношения в информационной сфере, а также недостаточная правоприменительная практика" — (8,9%).

Таким образом, на указанные 4 источника приходится в среднем по 9,4% значимости, а на остальные 13 — почти в два раза меньше, по 4,8%.

Для множества угроз наблюдается еще более характерная дифференциация. И, несмотря на то, что в отличие от источников угроз, индивидуальные оценки которых в силу независимости по определению допускают аддитивный способ учета совместного влияния, а здесь, за счет взаимозависимости, оно несколько ниже простой суммы индивидуальных оценок, 7 наиболее весомых элементов из 34 дают уже более половины (54%) значимости:

- (31) "Монополизация информационного рынка России, его отдельных секторов отечественными и зарубежными информационными структурами";
- (34) Противодействие доступу Российской Федерации к новейшим информационным технологиям, взаимовыгодному и равноправному участию российских производителей в мировом разделении труда …, а также создание условий для усиления технологической зависимости России в области современных информационных технологий";
- (19) "Создание монополий на формирование, получение и распространение информации в Российской Федерации, в том числе с использованием телекоммуникационных систем";
- (36) "Вытеснение с отечественного рынка российских производителей средств информатизации, телекоммуникации и связи";
- (27) "Вытеснение российских информационных агентств, средств массовой информации с внутреннего информационного рынка и усиление зависимости духовной, экономической и политической сфер общественной жизни России от зарубежных информационных структур";
- (35) "Закупка органами государственной власти импортных средств информатизации, телекоммуникации и связи при наличии отечественных аналогов, не уступающих по своим характеристикам зарубежным образцам";
- (37) "Увеличение оттока за рубеж специалистов и правообладателей интеллектуальной собственности".

Каждый из этих 7 видов угроз в среднем оценивается по 7,7%, в то время как все остальные 27 видов в среднем имеют оценку 2,3%, то есть в три с лишним раза меньше.

Как видно, список наиболее значимых элементов довольно правдоподобен, хотя исходные данные использовались весьма приблизительные. Это обстоятельство свидетельствует, с одной стороны, о том, что "Доктрина" достаточно полно представляет рассматриваемую проблему, а с другой — об адекватности использованной для расчетов модели.

Для мер по обеспечению защищенности национальных интересов РФ в информационной сфере, предлагаемых "Доктриной" (см. табл. 4 и рис. 5), был проведен расчет потенциальной результативности их реализации в полном объеме. Для первого (равновесного) варианта расчета исходная локальная результативность r_i для каждой из мер условно принималась равной 0,3. Тем не менее, показатель общей результативности r_z при этом составил 0,82, то есть более 80%. Однако, как видно на рис. 7, предлагаемые меры повышения уровня защищенности, рассчитанные относительно отдельных факторов, не достаточно целенаправленны с точки зрения воздействия на наиболее значимые из них, что говорит о возможности уточнения положений "Доктрины".

Труды СПИИРАН. 2002. Вып. 1. Т. 1. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2002. Issue 1. V. 1. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

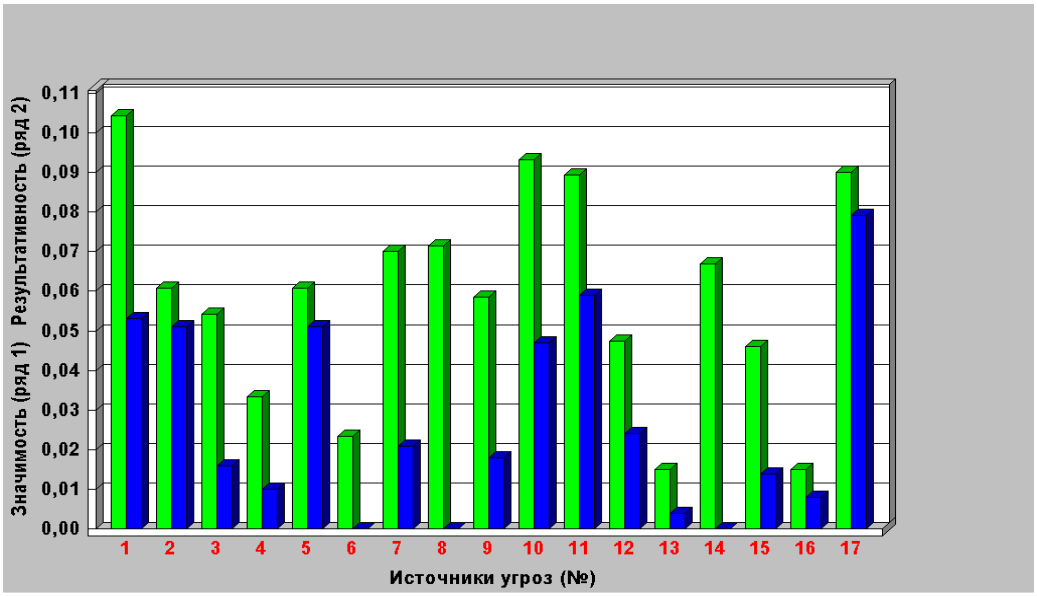

Рисунок 7. Диаграмма соотношения значимости источников угроз и результативности противодействий

Кроме мер, определенных "Доктриной", был также рассмотрен и оценен неявным образом содержащийся в [4] (далее — "Белая книга") альтернативный вариант воздействий, изменяющих состояние защищенности интересов РФ в информационной сфере. Табл. 5 содержит возможный их список, а на рис. 8 показана матрица отношений, аналогичная представленной на рис. 5 для "Доктрины". Знак минус у ненулевых элементов в матрице обозначает, что соответствующие им параметры r_i<0.

Расчеты показали, что при реализации некоторых мер, предлагаемых в "Белой книге", возможно следующее (для простоты полагалась равнозначность всех мер). При $r_{i=}$-0,1, что соответствует незначительному, на 10%, усилению действия факторов, на которые производятся локальные воздействия, интегральная результативность $r_{z=}$-0,76, и $s_{z=}$0,57, то есть защищенность интересов РФ в информационной сфере уменьшится почти в 2 раза. При доведении r_i до -0,2 соответствующие оценки $r_{z=}$-1,65, и $s_{z=}$0,38.

Рассмотрен также вариант совместной реализации мер ("Химера"), предлагаемых в "Доктрине" и в "Белой книге", являющийся условным, так как практически, в силу взаимоисключающего характера некоторых их положений, едва ли возможен. Тем не менее, полученные оценки представляют интерес. Исходные данные для "Доктрины" были взяты те же, что для проиллюстрированных на рис. 6 и рис. 7 расчетов, а для "Белой книги" рассмотренные выше два варианта значений r_i. Значения r_z получились соответственно равными 0,53 и 0,05, то есть, если при менее активной реализации положений "Белой книги" результативность предлагаемых "Доктриной" мер снизится примерно в полтора раза, то некоторая интенсификация их продвижения сведет эту результативность практически к нулю. Полученные результаты сопоставлены на рис. 9.

Труды СПИИРАН. 2002. Вып. 1. Т. 1. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2002. Issue 1. V. 1. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

Таблица 5. Некоторые меры по развитию информационных технологий в РФ [4].

#	Содержание мер
1.	Ориентация на сборочные технологии, отказ от собственных технологических разработок и развития элементной базы: "…недопустимость внедрения национальных стандартов, несовместимых с общепринятыми международными стандартами" (п.2.1.2); "…бессмысленность вложений в… современные, но высокозатратные производства с очень высокими показателями производительности труда"; "место России в мировом разделении труда на рынке информационных технологий - низкозатратные производства,…к таким производствам … не относится … производство микропроцессоров." (п.2.2.4).
2.	"…либерализация в области регулирования разработки, производства, распространения и использования средств защиты информации." (п.3.2.3.4).
3.	Отказ от культурных традиций народов РФ: "…глобализация мирового информационного пространства приводит к… культурной унификации общества на мировом уровне."; "…культурные традиции входят в противоречие с информационной открытостью и глобализацией." (п.3.2.4.2).
4.	"…снятие барьеров к внедрению информационных технологий в государственных органах" (п.3.2.4.3)
5.	Приоритетность английского языка перед языками народов РФ: "…незнание английского языка приводит к неконкурентоспособности на мировом рынке труда."; "…актуальность создания системы … массового обучения граждан …английскому языку." (п.3.2.4.1).
6.	Нежелательные: "прямое участие государства в экономике" (п.5.1).
7.	Нежелательные: "государственный протекционизм и защита отечественного производителя посредством тарифной политики" (п.5.1).
8.	Нежелательные: "усиление регулирующего воздействия государства в области лицензирования и сертификации продуктов и услуг" (п.5.1).
9.	Нежелательные: "введение искусственных ограничений на кадровую миграцию" (п.5.1).
10	Нежелательные: "введение контроля над информационными потоками" (п.5.1).

Воздействия	Источники угроз: внешние 1	2	3	4	5	6	7	внутренние 8	9	10	11	12	13	14	15	16	17	Угрозы: I 18	19	20	21	22	23	24	25	26	27	28	29	30	II 31	32	33	III 34	35	36	37	IV 38	39	40	41	42	43	44	45	46	47	48	49	50	51
1	0	-1	0	0	-1	0	-1	-1	0	0	0	0	0	0	-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	-1	0	-1	-1	0	0	-1	-1	0	-1	-1	-1	0	-1	-1	0
2	-1	0	0	0	0	-1	-1	0	-1	-1	0	0	0	0	0	0	0	0	0	-1	0	0	0	0	-1	0	0	0	0	0	0	-1	0	0	-1	-1	0	-1	0	0	-1	-1	-1	0	0	-1	-1	-1	-1
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	-1	-1	-1	-1	-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	-1	0	0	0	0	-1	-1	0	-1	0	-1	-1	0	0	-1	-1	0	-1	-1	-1
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	-1	-1	-1	0	0	0	0	0	0	0	0	0	-1	0	0	0	0	0	0	0	0	0	0	0	0
6	0	-1	0	0	0	0	0	0	-1	-1	-1	-1	-1	-1	0	0	0	0	-1	0	0	0	0	0	0	0	-1	0	0	0	-1	0	0	-1	0	-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	0	-1	0	0	-1	0	-1	-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	-1	0	0	0	-1	0	0	-1	-1	-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	-1	-1	0	-1	-1	0	-1	0	0	-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	-1	-1	-1	-1	0	0	0	-1	-1	0	-1	-1	-1
9	-1	0	0	0	-1	0	0	-1	0	0	0	0	0	0	-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	-1	0	0	0	0	0	0	0	0	0	0	0	0	0
10	0	0	0	-1	0	0	-1	0	-1	0	0	0	0	0	0	0	0	0	0	-1	0	-1	0	0	0	-1	-1	-1	0	-1	0	-1	0	0	0	0	0	-1	0	0	0	0	0	0	-1	0	0	-1	0	-1

Рисунок 8. Матрица отношений "меры - факторы" ("Белая книга")

Труды СПИИРАН. 2002. Вып. 1. Т. 1. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2002. Issue 1. V. 1. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

Рисунок 9 Соотношение результатов от реализации мер, изменяющих состояние защищенности национальных интересов РФ в информационной сфере

4. Заключение

Результаты исследования с уверенностью позволяют сделать вывод о безусловной актуальности и значительном аналитическом потенциале "Доктрины". Несмотря на некоторую условность количественных исходных данных, что определялось экспериментальным характером проделанной работы, она оказалась вполне конструктивной и показала возможность использования разработанных средств для поддержки собственного развития "Доктрины", и, особенно, в практическом плане, в качестве инструмента поддержки принятия решений в сфере обеспечения информационной безопасности, как на концептуальном, так и на инженерном уровнях.

Литература

[1] Юсупов Р. М., Заболотский В. П. Научно-методологические основы информатизации. - СПб.: Наука, 2000. - 455 с.

[2] Доктрина информационной безопасности Российской Федерации. 9 сентября 2000 г. № Пр-1895. - http://www.scrf.gov.ru/Documents/Decree/09-09.html

[3] Шишкин В. М. Концептуальная модель оценивания защищенности объектов информатизации, опыт использования в учебном процессе //"Информатика - исследования и инновации". Сб.научных трудов. ЛГОУ им.А.С.Пушкина. - СПб: 2000. - С. 114-116.

[4] "Белая книга информационных технологий". Проект рабочей группы Экспертного совета по информационным технологиям при Администрации Президента Российской Федерации. 29 декабря 2000 г. - http://www.libertarium.ru/libertarium/df_whitebook