УДК 37

ИНФОРМАЦИОННАЯ СФЕРА КАК СОВРЕМЕННЫЙ ПРИОРИТЕТ СРЕДЫ ОБИТАНИЯ ЧЕЛОВЕКА[1]

INFORMATION SPHERE AS A MODERN PRIORITY HUMAN ENVIRONMENT[2]

И.С. Шаповалова
I.S. Shapovalova

Белгородский государственный национальный исследовательский университет,
Россия, 308015, г. Белгород, ул. Победы, 85
Belgorod State National Research University, 85 Pobeda St, Belgorod, 308015, Russia

E-mail: shapovalova@bsu.edu.ru

Ключевые слова: среда обитания человека, информационная сфера, виртуализация сознания, коммуникативный капитал, информационные риски.
Key words: human environment, information sphere, virtualization of consciousness, communicative capital, information risks.

Аннотация. В статье рассмотрена нарастающая актуальность и значимость информационной в сферы в современной среде обитания человека с позиции научного дискурса, внимания общественности и диалога международного сообщества. Предложен анализ результатов всероссийского исследования, позволяющий оценить весомость существующих информационных угроз и рисков, в свете существующих тенденций экспансии процессов информатизации. В результате исследования определены наиболее значимые угрозы и риски информационной среды для существующих экономических сфер, обозначены факторные поля, катализирующие реализацию угроз. Определена востребованность управленческих мер и выделены наиболее эффективные меры регулирования информационных рисков среды обитания человека.
Resume. The article describes the growing relevance and significance of information in the sphere in the modern human environment from a position of scientific discourse, dialogue and public awareness of the international community. We propose an analysis of the results nationwide study, allowing to estimate the weight of existing information threats and risks in the light of current trends the expansion of informatization. The study identified the most significant threats and risks to information environment existing economic areas designated field factor catalyzing the implementation of threats. Determined demand management measures, and the most effective measures to control information risks of the human environment.

Информационная сфера, как неотъемлемая часть технического прогресса, занимает ведущее место в конструировании современной среды обитания человека. Являясь элементом техносферы, в силу существующих эволюционных тенденций, она выделяется в самостоятельную среду, имеющую собственную историю и траекторию развития.

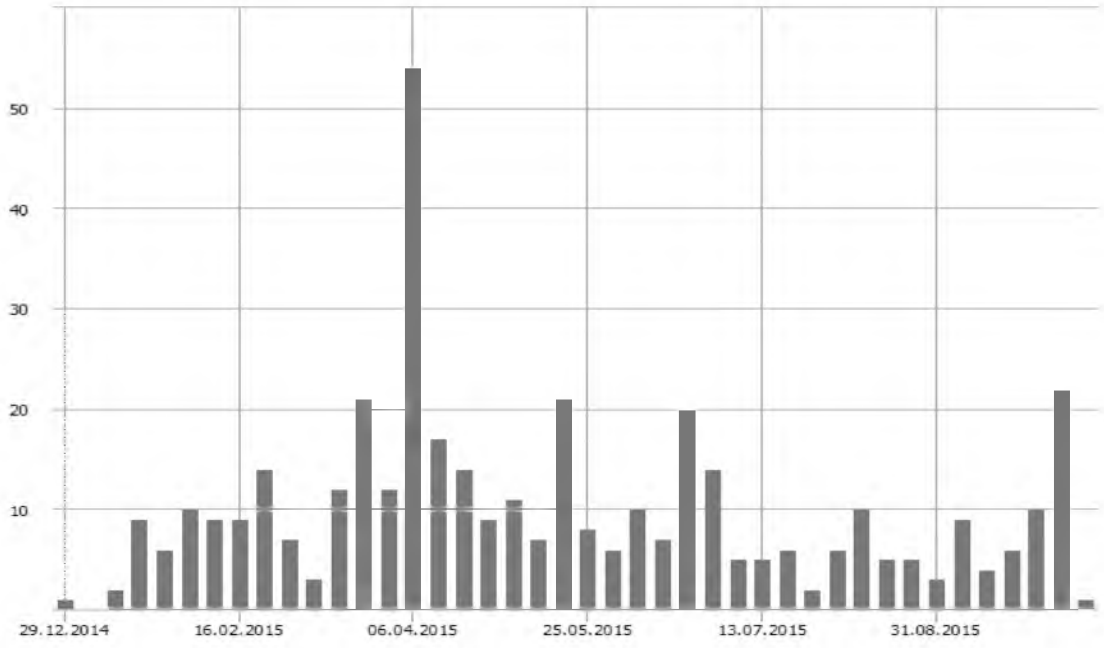
Рассматривая информационную сферу и ее процессы как часть техноэволюции [Цветков, 2005], в последнее время все больше исследователей склоняются к восприятию информатизации, как основного процесса инфосферы, в качестве условия эволюции общества, условия его перехода от индустриальной формы организации к информационной [Лонский, 2015]. Ученые, обращающиеся к исследованиям данной сферы, продуцируют теории и предлагают аналитику, демонстрирующую читателю специфические закономерности, сферные тенденции и уникальные риски [Завлин, 2003; Уэбстер, 2004; Шаповалова, 2015 и др.], весомость которых, при воплощении в реальность, способна «сместить полюса» человеческой эволюции, придав техносферным объектам субъектный статус [Шаповалова, Алексеенко, 2015]. Футурологические сценарии экстраполяции современных тенденций информационной сферы широко представлены в работах Н. Бострома, В. Виндж, Э. Тоффлер, Е. Юдковски и др. [Бостром, 2002; Виндж, 2004; Тоффлер, 2008; Юдковски,, 2008; и др.].

Внимание общества к информационной сфере, ее развитию и рискам, привлекается также посредством средств массовой информации. Только за последний год по данной тематике можно выделить более 400 публикаций, касающихся рисков информатизации (диаграмма 1).

[1] Исследование выполнено за счет гранта Российского научного фонда, проект №14-38-00047«Прогнозирование и управление социальными рисками развития техногенных человекомерных систем в динамике процессов трансформации среды обитания человека».
[2] This research was supported by research grant of Russian Science Foundation, project No 14-38-00047 "Forecasting effort and social risks management of anthropogenic human-caused systems development over time human environment transformation processes".

Диаграмма 1
Diagram 1

Динамика публикаций СМИ по проблемам и рискам развития информационной сферы
The dynamics of media publications on the problems and the risk of development of information sphere



Анализируя тематику выше обозначенных публикаций, можно уточнить, что наибольшее внимание привлечено к темам, связанным с информационными рисками в области социальных отношений (например, информатизации общества и населения, информационное неравенство), политики и государства (информатизация процесса управления, информационные войны), коммерческая деятельность (создание и коммерциализация информационного продукта) и др. (таблица 1).

Таблица 1
Table 1

Тематика публикаций СМИ по проблемам развития информационной сферы
The subjects of media publications on the development of the information sector

Наименование темы	**количество**
Социальные вопросы	70
Политика и государство	65
Сделки, проекты, инвестиции	62
Госрегулирование	58
Производственная деятельность	53

Информационная сфера, ее проблемы, угрозы и риски становятся темой для обсуждения и международного сообщества, в которое включаются, помимо ученых, представители власти и производства. Так, только за последние несколько лет, проведено большое количество знаковых научно-практических мероприятий, в числе которых можно упомянуть: Генеральная Ассамблея ООН, на которой Россия, Китай, Узбекистан, Таджикистан совместно предложили нормы международных действий в области информационной безопасности (ноябрь, 2011); Международная конференция в Лондоне по вопросам кибербезопасности (ноябрь, 2011); Международная конференция по киберпространству в Будапеште (октябрь, 2012); Международная конференция Международного союза электросвязи (ITU) в Дубае (декабрь, 2012); Международная конференция по кибервопросам в Сеуле (ок-

тябрь, 2013); Net Mundial в Сан-Паулу, Бразилия (апрель, 2014); Всемирная конференция по интернету в г. Вуджень, Китай (ноябрь, 2014).

Несмотря на попытки выработать единый взгляд по вопросам информационной безопасности и регулирования информационной экспансии, до сих пор существует ряд острых моментов, не просто не снижающих напряженности в информационной сфере, но и продуцирующих дополнительные, реальные и потенциальные угрозы данной сферы среды обитания человека. Большая часть таких разногласий отмечается в сфере регулирования информационного (кибер) пространства. Так, позиция США, Европы и Японии склоняется к тому, что государство не должно контролировать киберпространства, сохраняя принципы демократии как of– lain, так и on-lain. Россия, страны постсоветского пространства и Китай предполагают необходимость государственного регулирования киберпространства, подчеркивая уважение к суверенитету государства в нем. На данный момент трудно прогнозировать, чья позиция приведет к более эффективному итогу и как она трансформируется в общественном устройстве будущего.

В развитие данной темы Центром социологических исследований НИУ «БелГУ» в рамках выполнения проекта Российского научного фонда «Прогнозирование и управление социальными рисками развития техногенных человекомерных систем в динамике процессов трансформации среды обитания человека» был проведен всероссийский экспертный опрос. Исследование проведено сотрудниками совместной научно-исследовательской лаборатории трансдисциплинарных исследований (НИУ «БелГУ», ИСПИ РАН, ЮЗГУ). Целью экспертного опроса стала экспертиза информационных угроз, причин и возможностей предотвращения ситуаций нарушения информационной безопасности в регионах.

Опрос был проведен в период с 30 апреля по 1 июня 2015 г., общее количество экспертов, участвовавших в исследовании составило 120 человек. В качестве критериев отбора экспертов использовались сфера деятельности, опыт работы в сфере, способность (компетентность) оценивать ситуацию и прогнозировать ее развитие. Характеристика экспертной группы – профильные специалисты отраслевых организаций, административные работники и государственные служащие, сотрудники профильных кафедр высших учебных заведений и НИИ, специалисты общественных организаций. В качестве территориальной принадлежности были отобраны 8 регионов, которые были распределены по группам с различным уровнем рискогенности («уровень техногенной безопасности») на основании данных ГУ МЧС России, были выделены регионы РФ с максимальным и минимальным уровнем техногенного риска: Адыгея, Амурская область, Брянская область, Карачаево-Черкессия, Кировская область, Костромская область, Краснодарский край, Нижегородская область, Саратовская область, Тверская область.

Анализ экспертного мнения о вероятности возникновения угроз, связанных с информационными чрезвычайными ситуациями (ИЧС), показывает следующее их распределение по анализируемым территориям (диаграмма 3). В техносфере регионов наиболее часто возникают опасности и угрозы, связанные с нарушением прав интеллектуальной собственности (50,0%), что отражает современные тенденции как повышения значимости интеллектуального продукта, так и правовой грамотности населения. Наиболее редким явлением в современной информационной среде эксперты считают инциденты, связанные с неконтролируемым развитием глобальных информационных систем (так, на отсутствие таких ситуаций указали 65% экспертов).

Расчет индекса вероятности возникновения позволяет ранжировать информационные чрезвычайные ситуации (см. табл. 1)[3]. В тройку наиболее вероятных ИЧС входят технические сбои в работе каналов передачи информации (индекс вероятности 61,65), нарушение прав интеллектуальной собственности (34,95), незаконное проникновение в информационные системы, в том числе посредством сети интернет (28,35). Наименее вероятные ситуации, по мнению экспертов, связаны с неконтролируемым развитием глобальных информационных систем (-46,6), с авариями и нарушениями в системах хранения информации (-25,9).

Как показал экспертный опрос, в случае ИЧС массового информирования населения практически не осуществляется (17,2%). Чаще всего коммуникации происходят посредством донесения информации до непосредственных участников событий (41,4%) или специалистов (37,9%). Возможно, такие варианты распространения информации являются преимущественными по причине вторичности угроз информационного плана. Информационные угрозы на данный момент являются перспективным полем проблем, чей выход на первый план будет взаимосвязан со скоростью виртуализации массового сознания и кибертуализации социально-экономических процессов.

[3] Индекс рассчитывается, как разница между долями встречающихся информационных чрезвычайных ситуация и долями не встречающихся. При этом, долям ситуаций, часто встречающихся и никогда не встречающихся присваивается коэффициент 1, а встречающимся иногда – коэффициент 0,5.

Диаграмма 3
Diagram 3

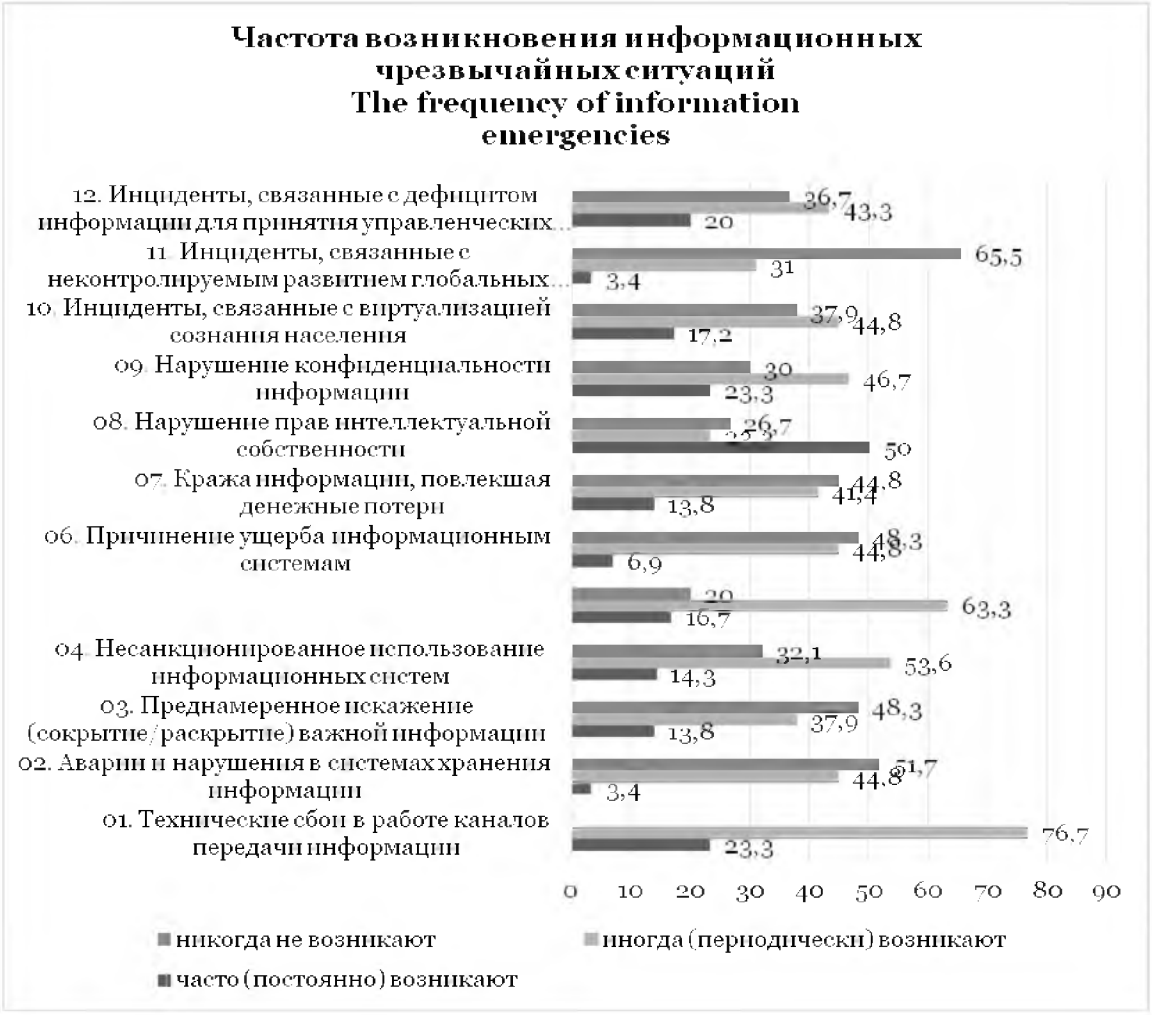


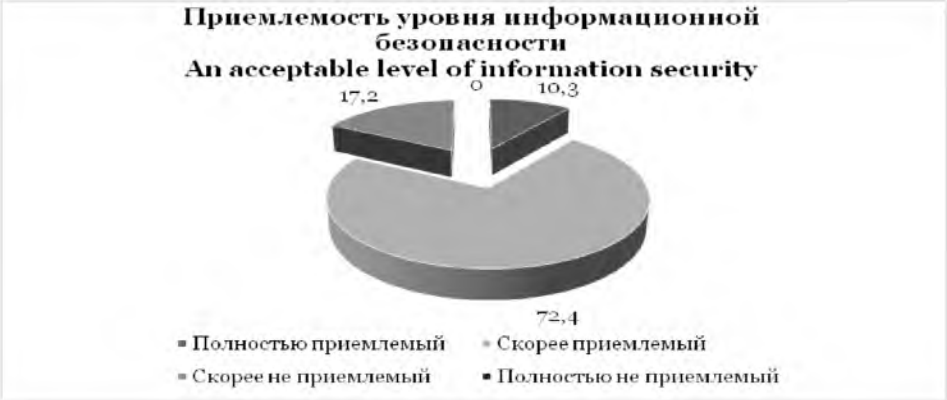
Таблица 2
Table 2

Ранжирование информационных чрезвычайных ситуаций по индексу вероятности их возникновения
Ranking Information emergencies the index of probability of their occurrence

Чрезвычайные ситуации в информационной сфере	Индекс вероятности возникновения	Ранг
Технические сбои в работе каналов передачи информации	61,65	1
Аварии и нарушения в системах хранения информации	-25,9	11
Преднамеренное искажение (сокрытие/раскрытие) важной информации	-15,5	9
Несанкционированное использование информационных систем	9,0	5
Незаконное проникновение в информационные системы, в том числе посредством сети интернет (хакерские атаки)	28,35	3
Причинение ущерба информационным системам	-19,0	10
Кража информации, повлекшая денежные потери	-10,3	8
Нарушение прав интеллектуальной собственности	34,95	2
Нарушение конфиденциальности информации	16,65	4
Инциденты, связанные с виртуализацией сознания населения	1,7	7
Инциденты, связанные с неконтролируемым развитием глобальных информационных систем	-46,6	12
Инциденты, связанные с дефицитом информации для принятия управленческих решений	4,95	6

Оценивая соотношение между допустимым уровнем информационной безопасности и экономическими возможностями его достижения, эксперты сделали выводы о приемлемости существующего в регионах уровня информационных рисков. Так 72,4% посчитали его скорее приемлемым, что совокупно с группой экспертов (10,3%) отметивших его однозначную приемлемость, составляет достаточно высокий показатель удовлетворенности уровнем информационной безопасности – 82,7%. 17,2% указали ту или иную степень неприемлемости существующей ситуации в информационной сфере регионов (диаграмма 4).

Диаграмма 4
Diagram 4



Сопряжение конкретных ИЧС с уровнем их приемлемости (для анализа взяты ситуации, встречающиеся не менее 1 раза в год), показало следующие результаты (диаграмма 5).

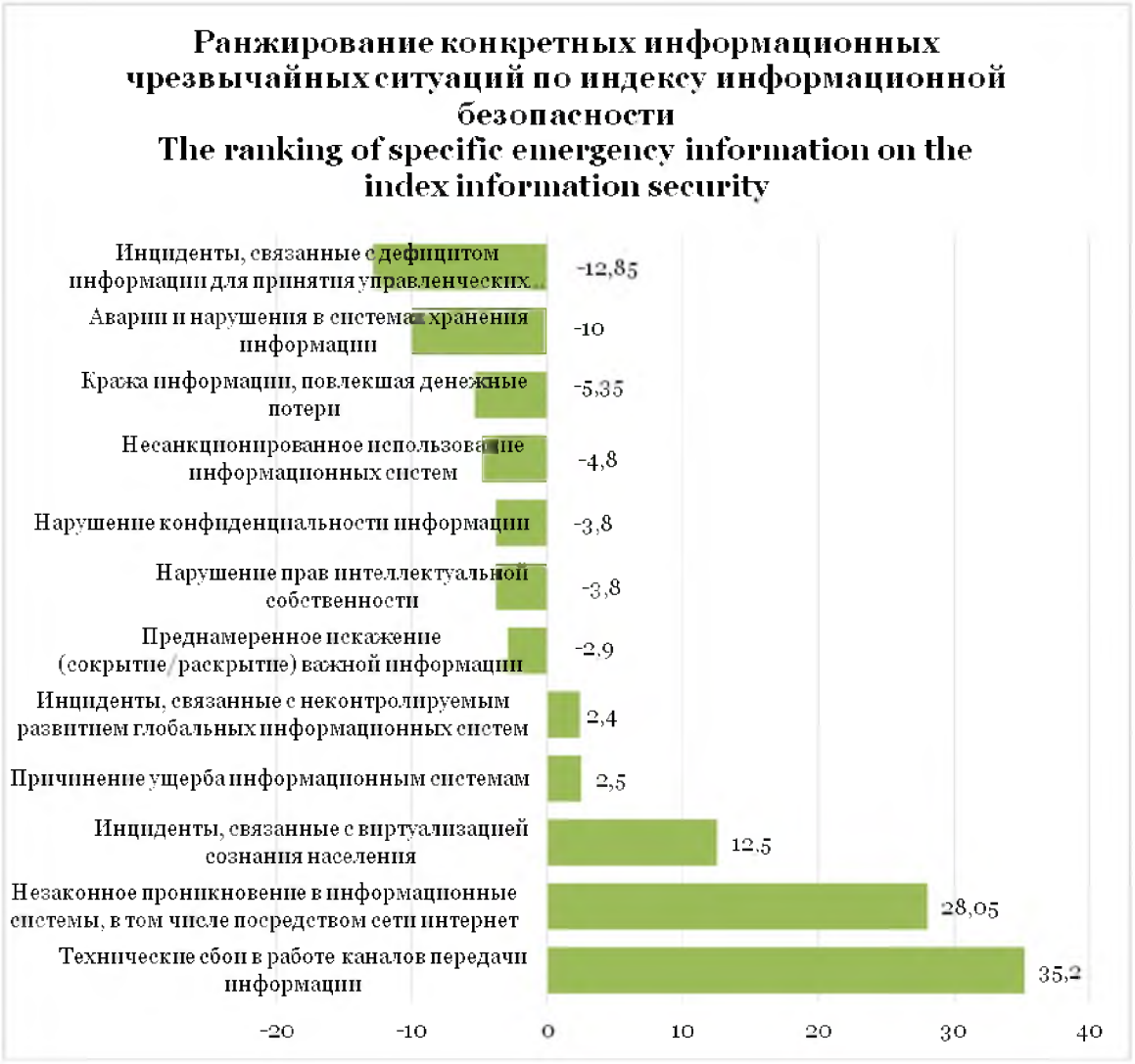
Диаграмма 5
Diagram 5

Так, 33,3% экспертов отмечают полную приемлемость с точки зрения информационной угрозы ситуаций, связанных с незаконным проникновением в информационные системы и с техническими сбоями в работе информационных систем. В отношении остальных ИЧС наблюдается та или иная степень приемлемости или ее отсутствие. Чаще других с точки зрения проблем упоминаются ситуации, связанные с нарушением конфиденциальности информации и нарушением прав интеллектуальной собственности (60,0%).

Расчет индекса информационной безопасности для конкретной ЧС, позволяет выделить группы наиболее опасных, с точки зрения частоты и приемлемости риска ситуаций и проранжировать их по этому показателю (диагр. 6).

Согласно показателям индекса, только одна из предложенных экспертам ситуаций может соответствовать приемлемому уровню безопасности – это технические сбои в работе каналов передачи информации (индекс имеет среднее значение 32,5). Также достаточно высокий показатель по индексу имеют ситуации, связанные с незаконным проникновением в информационные системы (28,05). В остальных случаях его можно оценить, как низкий или отрицательный. Наибольший показатель *опасности* наблюдается по инцидентам, связанным с дефицитом информации для принятия управленческих решений (-12,85), с авариями и нарушениями в системах хранения информации (-10,0).

Диаграмма 6
Diagram 6



Анализируя представленные в исследуемых регионах сферы и наличие в них конкретных информационных угроз, становится возможным установить связанные группы отрасль-угроза.

1) городской транспорт – инциденты, связанные с дефицитом информации для принятия управленческих решений;

2) легкая и пищевая промышленность, железнодорожный транспорт, автомобильный транспорт, магистральный трубопроводный транспорт, авиационные транспорт – нарушение прав интеллектуальной собственности;

3) строительство и промышленность строительных материалов – инциденты, связанные с дефицитом информации для принятия управленческих решений; несанкционированное использование информационных систем; нарушение прав интеллектуальной собственности;

4) деревообрабатывающая промышленность – нарушение прав интеллектуальной собственности; инциденты, связанные с дефицитом информации для принятия управленческих решений;

5) черная, цветная металлургия, нефтеперерабатывающая, нефтедобывающая, угольная промышленность, электроника, сельское хозяйство и рыболовство, морской транспорт, внутренний водный транспорт – нарушение конфиденциальности информации, нарушение прав интеллектуальной собственности.

Группы проблемных связок позволяют очертить «системные проблемы», характерные для большинства отраслей и регионов. К таковым относятся уже отмеченные ранее нарушение конфиденциальности информации и нарушение прав интеллектуальной собственности.

Диаграмма 7
Diagram 7

Оценивая высокую степень влияния информационных факторов на рискогенные области техносферы, наличие ситуаций информационного риска, эксперты установили, что более всего зависят от ИЧС отрасли, связанные с электроэнергетикой (77,30%), железнодорожный и авиационный транспорт (59,10% и 50,0% соответственно) (диаграмма 7). Менее других зависят от ИЧС сельское хозяйство и рыболовство, лесная и деревообрабатывающая промышленность, внутренний водный транспорт, черная металлургия и угольная промышленность (по 9,10% соответственно). Можно предполо-

жить, что наличие или отсутствие зависимости обусловлено уровнем и этапом информатизации отрасли. Принимая информатизацию одной из ведущих, глобальных, современных тенденций, можно сделать гносеологический вывод о каузальных связях между степенью зависимости отрасли от информационной сферы и уровнем ее прогрессивного развития.

Степень влияния рискогенных факторов информационного локуса среды обитания по оценкам экспертов распределилась по шкале оценки следующим образом (см. табл. 3). Все эксперты наиболее значимой группой признали факторы, связанные с человеком (средняя оценка по семибалльной шкале 5,47) и недостаточное внимание собственника к обеспечению информационной безопасности (5,27). Наименьшее влияние эксперты определили для факторов, связанных с природой и техносферой (2,50 и 2,63).

Таблица 3
Table 3

Оценка влияния рискогенных факторов информационного локуса на возникновение информационных чрезвычайных ситуаций в среде обитания человека
Assessing the impact of risk– taking factors locus information on the occurrence of emergency information in the human environment

Информационные рискогенные факторы	N	Минимум	Максимум	Среднее	Стд. отклонение
Связанные с изменением со временем свойств информационных систем	30	1	7	4,57	1,736
Связанные с появлением новых, неизученных на момент внедрения, свойств информационных систем	30	1	7	4,67	1,845
Связанные с недостатком информации о состоянии безопасности информационной сферы	30	1	7	4,63	1,712
Человеческий фактор	30	1	7	5,47	1,676
Недостаточное внимание собственника к обеспечению информационной безопасности	30	2	7	5,27	1,437
Влияние природных факторов	30	1	6	2,50	1,526
Социокультурные факторы	30	1	7	4,27	1,799
Состояние правовой и законодательной базы по обеспечению информационной безопасности	30	1	7	3,83	2,001
Влияние техносферы	30	1	5	2,63	1,129
Недостатки в управлении	30	1	7	4,07	1,889

Расчет коэффициентов корреляции между влияющими факторами позволяет определить наиболее устойчивые факторные группы (таблица 4):

– Факторы, связанные с изменением со временем свойств информационных систем, объединяются с группой факторов, связанных с появлением новых свойств информационных систем, с человеческим и природным фактором;

– Факторы, связанные с появлением новых, неизученных на момент внедрения, свойств информационных систем, объединяются с группой факторов, связанных с влиянием техносферы, с человеческим и природным фактором;

– Факторы, связанные с недостатком информации о состоянии безопасности информационной сферы, объединяются с группой факторов, связанных с человеческим и социокультурным факторами;

– Факторы, связанные с влиянием природной сферы, объединяются с группой факторов, связанных с состоянием правовой и законодательной базы;

– Социокультурные факторы объединяются с группой факторов, связанных с влиянием техносферы.

Сопряжение оценки значимости рискогенных факторов и возникновения конкретных чрезвычайных ситуаций дает возможность наглядно продемонстрировать каузальные связи и моделировать рискогенное факторное облако каждой из угроз. Для каждой угрозы инфосферы существуют свои информационные риски. Наиболее значимые из них оценены экспертами от 5 до 7 баллов.

Таблица 4
Table 4

Корреляционные связи факторов инфосферы
Correlation factors infosphere

Информационные рискогенные факторы	Изменение со временем свойств информационных систем	Появление новых, свойств информационных систем	Недостаток информации о состоянии безопасности информационной сферы	Человеческий фактор	Недостаточное внимание собственника	Влияние природных факторов	Социокультурные факторы	Состояние правовой и законодательной базы	Влияние техносферы
Связанные с изменением со временем свойств информационных систем	,717	,718	,285	,723	,283	,497	,356	,272	,415
Связанные с появлением новых, неизученных на момент внедрения, свойств информационных систем		,405	,421	,552	,274	,498	,200	,181	,472
Связанные с недостатком информации о состоянии безопасности информационной сферы			,213	,615	,358	,325	,466	,357	,297
Человеческий фактор				,154	,010	,377	,223	,252	,337
Недостаточное внимание собственника к обеспечению информационной безопасности					,065	,254	,190	,001	,216
Влияние природных факторов						,337	,363	,647	-,062
Социокультурные факторы							,297	,165	,499
Состояние правовой и законодательной базы по обеспечению информационной безопасности								,441	,212
Влияние техносферы									,204

Рискогенные факторные поля чрезвычайных ситуаций инфосферы представлены в таблице 5. В крайнем ее столбце дан показатель индекса рискогенной уязвимости, рассчитанный как доля совокупного влияния рисков инфосферы от максимально возможного влияния[4].

Исходя из данных таблицы 5 наиболее обусловлены влиянием информационных рискогенных факторов ситуации, связанные с авариями и нарушениями в системах хранения информации (индекс рискогенной уязвимости 0,85), с преднамеренным искажением важной информации (0,73). Наименее уязвимы к воздействию внешних рискогенных факторов инциденты, связанные с неконтролируемым развитием глобальных информационных систем (0,47).

Оценивая эффективность мер и их использование в обеспечении и повышении уровня информационной безопасности регионов, эксперты определили в качестве наименее используемых мер внедрение рыночных механизмов регулирования инфосферы и совершенствование методов управления информационными рисками в регионе (по 27,6% соответственно) (диаграмма 8).

Чаще всего, в качестве наиболее эффективных, отмечены меры: укрепление кадрами служб информационной безопасности (51,7%) и усиление мер контроля на всех стадиях разработки информационного продукта (48,3%). В качестве не эффективных мер часто упоминаются информирование населения об уровнях и причинах информационных рисков (26,7%).

Для получения более достоверных данных об эффективности предлагаемых к оценке мероприятий, была произведена индексация данных с последующим их ранжированием.

В целом, ранжируя меры по индексу эффективности на территории РФ, можно разделить их на эффективные (индекс 76-100), более эффективные (51-75), менее эффективные (26-50) и неэффективные (отрицательные значения и 0-25)[5] (диагр. 9).

[4] Исходя из выделенных 9 факторов риска, максимальная рискогенная уязвимость может быть равна 63 в балльном эквиваленте (что равно единице в долевом эквиваленте).

Таблица 5
Table 5

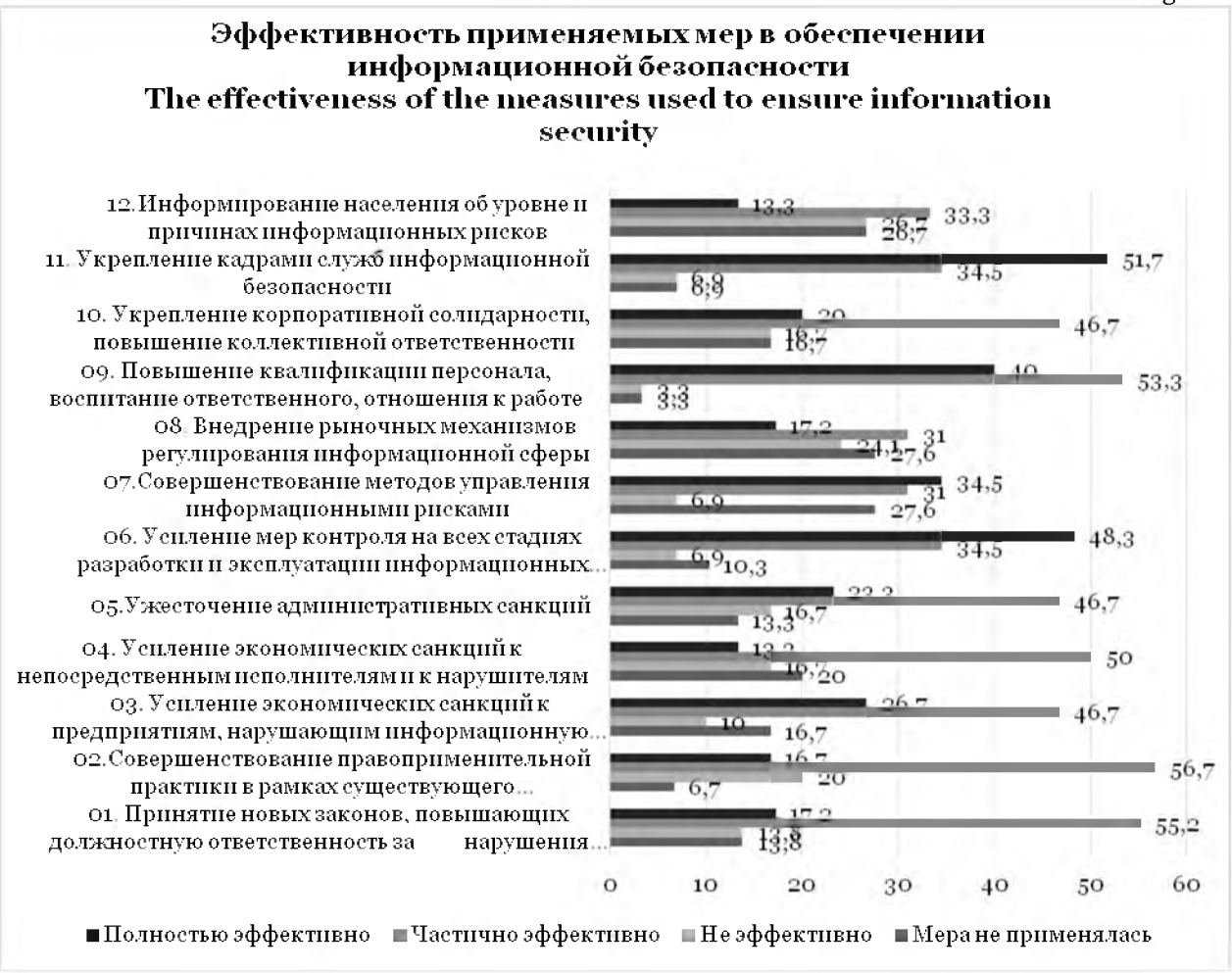
Рискогенные факторы инфосферы
Risk-taking factors infosphere

Информационные чрезвычайные ситуации	Изменение со временем свойств информационных систем	Появление новых, свойств информационных систем	Недостаток информации о состоянии безопасности информационной сферы	Человеческий фактор	Недостаточное внимание собственника	Влияние природных факторов	Социокультурные факторы	Состояние правовой и законодательной базы	Влияние техносферы	Недостатки в управлении	ИНДЕКС РИСКОГЕННОЙ УЯЗВИМОСТИ
Технические сбои в работе каналов передачи информации	4,43	5,29	4,57	6,29	5,43	2,71	5,57	4,14	2,43	4,43	**0,64**
Незаконное проникновение в информационные системы, в том числе посредством сети интернет	5,20	5,20	5,00	5,60	5,40	3,20	5,20	3,60	2,20	3,50	**0,55**
Инциденты, связанные с виртуализацией сознания населения	4,20	4,20	4,80	5,00	5,60	1,80	4,60	3,80	2,20	4,00	**0,57**
Причинение ущерба информационным системам	5,50	5,50	4,50	5,50	6,00	1,50	4,50	3,50	1,50	4,00	**0,6**
Инциденты, связанные с неконтролируемым развитием глобальных информационных систем	3,00	5,00	2,00	6,00	3,00	1,00	3,00	1,00	3,00	6,00	**0,47**
Преднамеренное искажение (сокрытие/раскрытие) важной информации	6,25	5,25	6,50	5,50	6,25	2,50	5,50	5,25	3,00	5,25	**0,73**
Нарушение прав интеллектуальной собственности	4,60	4,80	4,53	5,93	5,07	1,73	4,40	3,87	2,27	4,14	**0,59**
Нарушение конфиденциальности информации	5,00	5,14	4,71	6,57	4,71	2,14	5,00	5,00	2,57	4,57	**0,64**
Несанкционированное использование информационных систем	5,00	5,00	4,75	6,00	6,00	1,25	4,50	3,25	1,50	3,67	**0,58**
Кража информации, повлекшая денежные потери	4,50	5,25	4,25	6,50	5,25	2,50	5,00	4,25	2,50	3,75	**0,62**
Аварии и нарушения в системах хранения информации	7,00	7,00	7,00	7,00	5,00	3,00	7,00	6,00	4,00	7,00	**0,85**
Инциденты, связанные с дефицитом информации для принятия управленческих решений	5,00	4,17	6,00	4,83	5,17	2,33	4,00	5,33	2,67	4,00	**0,62**

По результатам индексации и ранжирования мер к группе эффективных мероприятий могут быть отнесены повышение квалификации персонала, воспитание ответственного, отношения к работе (индекс 63,35), укрепление кадрами служб информационной безопасности (62,05), усиление мер контроля на всех стадиях разработки и эксплуатации информационных систем (58,65). К самым неэффективным мерам могут быть определены информирование населения об уровне и причинах информационных рисков (3,25), внедрение рыночных механизмов регулирования информационной сферы (8,6).

[5] Индекс рассчитывается как разница между долей эффективны и относительно эффективных мер и мер неэффективных, при этом доля относительно эффективных мер умножается на 0,5, а доля неиспользованных мер не учитывается в расчете.

Диаграмма 8
Diagram 8



Таким образом, результаты анализа проведенного исследования акцентируют наше внимание на том, что наибольшей информационной опасностью, продуцируемой информационной сферой, для нас становится нарушение конфиденциальности информации и ущемление авторских прав на интеллектуальную собственность. Актуальность данных угроз подтверждается и активной законотворческой деятельностью не только в России, но и в других странах. Эта насущная проблема, видимая невооруженным глазом обычному пользователю, полностью затмевает перспективные угрозы футурологического толка – неконтролируемое развитие информационной сферы и связанные с этим уменьшение коммуникативного капитала, виртуализацию сознания, возникновение альтернативной реальности и др.

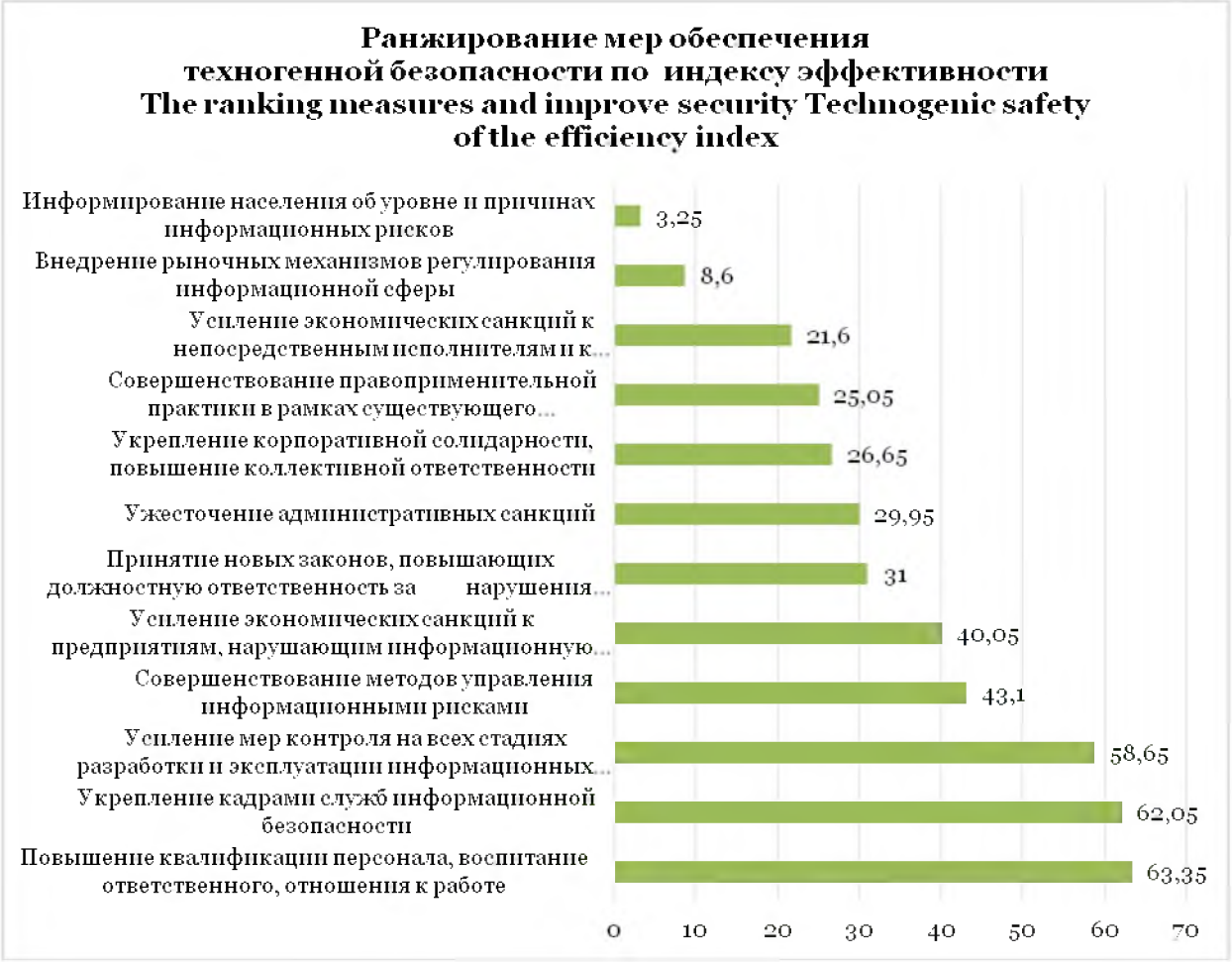
Хотя информационная сфера по праву занимает главенствующее положение в среде обитания человека, ее угрозы и опасности не воспринимаются как массовое бедствие и не относятся к разряду катастроф. Информационная безопасность и ее контроль привлекают внимание общественности скорее с позиции новостной информации, нежели с позиции жизнеопределющего фактора. В целом, несмотря на существующие тревожные мировые тенденции (информационный терроризм, информационные войны, кибершпионаж и т.д.), эксперты говорят о том, что уровень информационной безопасности в России можно охарактеризовать как приемлемый, с локализацией проблем в зоне принятия управленческих решений и хранения информации.

Мероприятия, предпринимаемые для нивелирования рисков и ингибирования угроз, которые можно условно считать наиболее эффективными, относятся скорее к группе локальных мер, в то время как их глобализация не находит отражение в комплексе информационной безопасности.

Сравнивая результаты диагностики угроз и рисков информационной сферы с другими компонентами среды обитания (природная сфера, социокультурная сфера, техносфера), создается ощущение видимого благополучия и нематериальности существующих угроз. Но, одновременно с этим, возникает понимание стохастичности развития информационных процессов. Реализация футурологиче-

ских прогнозов, даже в самом благоприятном их варианте, диктует необходимость углубленной диагностики рискогенных полей трансформации информационной сферы.

Диаграмма 9
Diagram 9



Список литературы
References

1. Виндж В. Технологическая сингулярность // Компьютерра. 2004.
Vindzh V. Tekhnologicheskaya singulyarnost' // Komp'yuterra. 2004.
2. Завлин П. Н. Некоторые проблемы инновационного развития // Инновации. Проблемы и опыт. 2003. № 5. URL: http:// www.mag.innov.ru (дата обращения: 15.09.2015).
Zavlin P.N. Some problems of innovative development // Innovatsii. Problemy i opyt. 2003. №. 5. URL: http://www.mag.innov.ru (accesed 15.09.2015).
3. Лонский И.И. Информатизация и эволюция общества // Перспективы Науки и Образования. 2015. № 2. С. 29-35.
Lonskii I.I. Informatization and the evolution of society // Perspectives of Science & Education. 2015. № 2. P. pp. 29-35.
4. Тоффлер Э. Шок будущего. М. 2008.
Toffler E. Shok budushchego. M. 2008.
5. Уэбстер Ф. Теории информационного общества. М. 2004.
Uebster F. Teorii informatsionnogo obshchestva. Moscow, 2004.
6. Цветков В.Я. Глобализация и информатизация // Информационные технологии. 2005. № 2. С. 2-4.
Tsvetkov V.Ia. Globalization and Informatization // Informatsionnye tekhnologii. 2005. №. 2, pp. 2-4.

7. Шаповалова И.С. Влияние интернет-коммуникаций на поведение и интеллектуальное развитие молодежи // Социологические исследования. 2015. № 4. С. 148-151.

Shapovalova I.S. Vliyanie internet-kommunikacij na povedenie i intellektual'noe razvitie molodezhi // Sociologicheskie issledovaniya. 2015. № 4. pp. 148-151.

8. Шаповалова И.С. Алексеенко А.И. Проблемы новых форм взаимодействия человека и техносферы // Социология религии в обществе Позднего Модерна. Белгород. 2015. С. 113-121.

Shapovalova I.S. Alekseenko A.I. Problemy novyh form vzaimodejstviya cheloveka i tekhnosfery // Sociologiya religii v obshchestve Pozdnego Moderna. Belgorod. 2015. pp. 113-121.

9. Юдковски Е. Систематические ошибки в рассуждениях, потенциально влияющие на оценку глобальных рисков. Новые технологии и продолжение эволюции человека? // Трансгуманистический проект будущего. М. 2008.

Yudkovski E. Sistematicheskie oshibki v rassuzhdeniyah, potencial'no vliyayushchie na ocenku global'nyh riskov. Novye tekhnologii i prodolzhenie ehvolyucii cheloveka? // Transgumanisticheskij proekt budushchego. M. 2008.

10. Bostrom N. Existential Risks: Analyzing Human Extinction Scenarios and Related Hazards // the Journal of Evolution and Technology. Vol. 9. 2002.