ИНФОРМАЦИОННЫЙ ВАНДАЛИЗМ, КРИМИНАЛ И ТЕРРОРИЗМ КАК СОВРЕМЕННЫЕ УГРОЗЫ ОБЩЕСТВУ

ОСИПОВ В.Ю., ЮСУПОВ Р.М.

УДК 351.75
Осипов В.Ю., Юсупов Р.М. **Информационный вандализм, криминал и терроризм как современные угрозы обществу.**
Аннотация. Дается краткий анализ состояния информационной безопасности общества. Формулируются актуальные научные проблемы, решение которых позволит снизить риски от информационного вандализма, криминала, терроризма. Предлагаются некоторые подходы к снижению остроты проблемы информационной безопасности.
Ключевые слова: информационный вандализм, криминал, терроризм, угрозы обществу, противодействие, проблемы, модели, методы, средства.

Osipov V.Yu., Yusupov R.M. **Information vandalism, crime and terrorism as modern threats to a society**.
Abstract. The brief analysis of society information safety condition is given. Actual scientific problems which decision will allow to lower risks from information vandalism, crime, terrorism are formulated. Possible approaches to decrease in an acuteness of a problem of information safety are offered.
Keywords: information vandalism, crime, terrorism, population threats, counteraction, problems, models, methods, means.

1. Введение. Характеристика угроз. Современному обществу свойственен ряд устойчивых тенденций. Имеет место активное развитие различных информационно-телекоммуникационных систем и средств с глобальным охватом населения Земли. Чем дальше, тем выше становится уровень информатизации общества.

Непрерывно расширяются возможности по предоставлению государственным структурам, бизнесу, законопослушным и асимметричным гражданам, группам различных функций по обращению с информацией. Это функции по доступу к накопленным мировым информационным ресурсам (ИР), формированию собственных ИР и оперативному предоставлению их широким слоям общества.

На граждан различных стран, городов, населенных пунктов через радио, телевидение, Интернет, газеты, журналы, книги, фильмы, компьютерные игры, обучение и общение идет нарастающий поток разнородной, зачастую противоречивой и недостоверной информации.

Увеличивается зависимость поведения населения от содержания этого информационного потока.

Такой поток на различных уровнях несет в себе как позитивную, так и деструктивную составляющую, приводящую к различным кон-

Труды СПИИРАН. 2009. Вып. 8. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2009. Issue 8. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

фликтам в обществе и попыткам их разрешить незаконным путем, реализацией асимметричных действий, наносящих существенный моральный и материальный ущерб.

В качестве деструктивной составляющей могут выступать:

- ложные сообщения об авариях на предприятиях промышленности (атомных электростанциях, химических заводах и других), о заминированных домах, поездах, самолетах, о финансовых крахах компаний, провокации и слухи в политической сфере;
- различного вида информация, вызывающая страх, агрессию, недовольство, раздражительность, порождающая сомнения, призывающая к деструктивным действиям;
- информационные сигналы, изменяющие психофизическое состояние людей, повышающие их утомляемость, вызывающие головные боли, повышающие давление и другие;
- деструктивные программы, как отрицательно влияющие на людей, так и дезорганизующие различные системы управления, вычислительные сети и технические средства и так далее.

Известно много случаев таких деструктивных воздействий, получивших большой резонанс в мире:

- первое поражение сети Интернет в 1988 году «сетевым червем» Роберта Мориса и последующие на нее атаки;
- передачи по отечественному телевидению специальных сигналов и видеоинформации в период перестройки и в настоящее время;
- показ по Японскому телевидению одной из серий про покемонов, спровоцировавшей приступы эпилепсии у детей;
- случаи насилия с применением оружия детьми после просмотра агрессивных и провоцирующих фильмов, участия в негативных компьютерных играх в развитых странах;
- публикация скандальных карикатур на пророка Мухаммеда датской газетой Jyllands-Posten в сентябре 2005 года, перепечатанных позже в газетах Норвегии (Magazinet), Франции (France Soir, Liberation, Le Monde), Германии (Die Welt), Испании (El Pais), Бельгии (De Standaard) и других;
- информационный вандализм и криминал со стороны различных сект;

Труды СПИИРАН. 2009. Вып. 8. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2009. Issue 8. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

- это, в какой-то мере, деструктивные информационные воздействия через средства массовой информации, спровоцировавшие мировой экономический кризис, и другие.

По экспертным оценкам величина ущерба от этих воздействий ежегодно в мире исчисляется в миллиардах и триллионах долларов.

Все эти деструктивные воздействия могут быть подразделены на мероприятия информационного вандализма, криминала и терроризма.

Информационный вандализм (ИВ) понятие довольно новое. Это одна из современных форм вандализма (умышленного и бессмысленного уничтожения, разрушения культурных, материальных ценностей и нематериальных активов). Происхождение слова «вандализм» связано с названием восточно-германского племени вандалов, разграбивших в июне 455 года Рим.

Под информационным вандализмом предлагается понимать деструктивные действия при обращении с различного рода информацией, не обусловленные террористическими и криминальными целями. Такой вандализм следствие безграмотности, любопытства, безответственности, непродуманной рекламы, некорректных высказываний по радио и телевидению, не осторожных публикаций карикатур, недостоверных порочащих фактов. Общая направленность ИВ – это разрушение имеющейся информационной среды. Несмотря, на первый взгляд, безобидность информационного вандализма, по масштабности он существенно перекрывает ИК и ИТ и наносит не меньший ущерб обществу, чем ИК и ИТ.

Информационный криминал (ИК) с учетом [1] – это действия отдельных лиц или групп, направленных на взлом систем защиты, на хищение, уничтожение, искажение информации, а также формирование (разработку) и распространение деструктивных информационных воздействий в корыстных или хулиганских целях. Он отличается от ИТ, прежде всего, целями. Формы реализации деструктивных действий у них практически одни.

Под информационным терроризмом (ИТ) понимается вид террористической деятельности, ориентированный на принуждение к реализации политических, экономических, религиозных, идеологических и других целей через деструктивные действия в сфере информации. Различают кибер-, телевизионный, телефонный, музыкальный и другие виды информационного терроризма. Одним из примеров современного кибертерроризма выступают события в Эстонии с 27 апреля по 18 мая 2007 года. В этот период сайты газет, основных банков и правительственных учреждений подвергались массированным бом-

Труды СПИИРАН. 2009. Вып. 8. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2009. Issue 8. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

бардировкам спамом или стали жертвами взломщиков. К телевизионному терроризму следует отнести освещение по соответствующим каналам выступлений террориста № 1, Бен-Ладена. Телефонный терроризм, явление очень распространенное во всех странах мира. Терроризируют не только отдельных лиц, но крупные государственные и коммерческие структуры взрывами, физической расправой и другими угрозами. Музыкальный терроризм предусматривает достижение террористическими организациями целей через деструктивные музыкальные произведения.

Информационный терроризм при внешнем сходстве по форме и методам с информационным криминалом отличается от него целями и тактикой проведения. Главное в тактике информационного терроризма состоит в том, чтобы террористический акт имел опасные последствия и получил широкий общественный резонанс. Как правило, требования террористов сопровождаются угрозой повторения террористического акта обычно без указания конкретного объекта и места действия.

Заметим, что способы и средства реализации мероприятий ИК и ИТ, как и ведения современной информационной войны, в настоящее время в мире, к сожалению, получили большое развитие [2–10].

Последствия ИВ, ИК и ИТ могут сказываться как на разрушении моральных устоев, поведении и конфликтности различных слоев населения, групп, отдельных лиц, так и на работе общественного транспорта, систем жизнеобеспечения, промышленных и социальных учреждений, телекоммуникационных и других сетей. Кроме этого скрытые деструктивные информационные воздействия на сознание широких слоев населения являются не только подпиткой уже сформированных асимметричных групп населения или отдельных граждан, но и порождения новых деструктивных структур. Все эти негативные предпосылки и проявления информационных асимметричных слабо контролируемых угроз уже не только существенно сказываются на состоянии всего человечества, но и чреваты для будущих поколений.

2. Состояние развития практики и теории противодействия. Анализ современных работ [11–19] по ИВ, ИК, ИТ свидетельствует, что исследования этих социальных явлений и мер противодействия им далеки от глубокой проработки. Имеются определенные результаты в области обеспечения информационной безопасности, прежде всего, технических, в меньшей мере, биологических систем. В целом, что касается населения, как объекта защиты от деструктивных информационных воздействий по различным каналам, здесь больше проблем, чем ответов.

Труды СПИИРАН. 2009. Вып. 8. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2009. Issue 8. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

В Российской Федерации в общем виде определены основные методы обеспечения информационной безопасности [17]. Отражены особенности ее в различных сферах общественной жизни (экономике, внутренней и внешней политике, области науки и техники, духовной жизни, общегосударственных информационных и телекоммуникационных системах, обороне). Однако реальное воплощение положений утвержденной доктрины информационной безопасности на практике связано с большими трудностями и даже негативными аспектами. В частности, из-за обеспечения технологической независимости и возможных информационных угроз введены существенные ограничения на использование импортного программного обеспечения и элементной базы при разработке ряда отечественной радиоэлектронной техники. С одновременным повышением информационной безопасности эти ограничения не только замедлили темпы развития этой техники, но и существенно увеличили затраты на ее создание. Вопрос о целесообразном соотношении между затратами на обеспечение информационной безопасности и возможными потерями для общества от информационных угроз остается открытым. Практика защиты информации на основе дорогих услуг не стимулирует прогресс. В тоже время аспекты противодействия ИВ, ИК, ИТ, связанные с оперативной проверкой информации на предмет информационно-психологической безопасности, остаются без должного внимания.

В определенной мере это обусловлено невысоким уровнем развития научной базы противодействия ИВ, ИК, ИТ не только в России, но и за рубежом.

Известны научно-методические подходы к такому противодействию [8, 13, 16, 19] и другие. В основном это методы на основе мнений экспертов и упрощенных математических моделей. Выход на многофакторные количественные оценки, предусматривающие наличие более адекватных математических моделей, осуществляется редко, за исключением, вопросов кибербезопасности, радиоэлектронной и криптозащиты. Традиционные методы цензурного характера в настоящее время существенно устарели из-за их инерционности и субъективности. В основном проблемами информационно-психологической безопасности по отношению к человеку, обществу занимались и продолжают заниматься специалисты в области общественных наук. Их техническая и методическая оснащенность, несомненно, возросла за последние годы. Разработаны специальные методики и стенды для анализа профессиональной психологической пригодности граждан, и в частности, для оценки влияния на них различного рода информацион-

Труды СПИИРАН. 2009. Вып. 8. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2009. Issue 8. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

ных воздействий. Однако методы и средства, позволяющие оперативно выявлять скрытую деструктивную информацию, без непосредственного ее воздействия на людей, в настоящее время практически отсутствуют.

Можно утверждать, что имеет место существенный разрыв между уровнем развития теории противодействия ИВ, ИК, ИТ и потребностями практики. Способы и средства деструктивного информационного воздействия на население существенно обогнали в своем развитии теорию и практику противодействия этим угрозам.

3. Формулировка и общая характеристика проблем противодействия. С учетом вышесказанного необходима разработка теории этих процессов, новых математических моделей и методов, позволяющих:

- эффективно прогнозировать деструктивные действия групп и лиц в условиях разнородной, неполной и зачастую недостоверной информации о них;
- оперативно выявлять и пресекать опасные информационные воздействия на население, передаваемые (переносимые) посредством различных носителей и средств, в том числе через средства массовой информации.

В перспективе это позволит разработать эффективные системы и средства оперативной проверки разнородной, прежде всего, семантической информации по требованиям безопасности, тем самым снизить возможные риски от информационного вандализма, криминала и терроризма, а также вырабатывать рекомендации по разрешению многих широкомасштабных конфликтов в обществе.

В интересах устранения имеющихся противоречий между уровнем развития науки и потребностями практики противодействия ИВ, ИК, ИТ предлагается решить ряд частных проблем:

1. Сформировать концептуальные модели ИВ, ИК, ИТ, как современных угроз человечеству. Необходимо уточнить понятия и категории, характерные ИВ, ИК, ИТ, глубже проанализировать цели, задачи, возможности и условия проявления этих явлений в Российской Федерации и в мире. Следует систематизировать возможные методы, средства и объекты, а также вскрыть причинно-следственные связи, порождающие ИВ, ИК, ИТ.

В определенной мере при решении этой частной проблемы можно опереться на известные результаты анализа террористических угроз [20–23] с учетом человеческого фактора [24–26], методы традицион-

Труды СПИИРАН. 2009. Вып. 8. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2009. Issue 8. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

ной радиоэлектронной борьбы [10] и ведения информационной войны [2, 5].

2. Разработать теоретические основы противодействия ИВ, ИК, ИТ. Желательно определить цели, задачи, методы и потенциальные средства такого противодействия. Нужна разработка соответствующей системы показателей и критериев оценки эффективности. Требуется математически сформулировать основные задачи противодействия, разработать методы их решения.

В основу этих исследований могут быть положены теоретические положения радиоэлектронной борьбы [10], комплексного технического контроля [10, 27], компьютерной безопасности [14].

3. Получить приемлемые для практики подходы к математическому моделированию поведения населения, социальных слоев, групп и конфессий, как объектов защиты от ИВ, ИК, ИТ. Необходимо разработать формализмы, отражающие основные свойства объектов защиты в условиях деструктивных информационных воздействий. Требуются математические модели, учитывающие структурную сложность, саморазвитие и перестройку этих объектов во времени, не только в зависимости от этих информационных воздействий, но и других факторов.

В частности для моделирования поведения объектов защиты можно использовать относительно-конечные операционные автоматы [28, 10], которые являются моделями перестраиваемых, перепрограммируемых систем. Отличие их от традиционных автоматов в том, что все их параметры, в том числе множества функций переходов и выходов, конечны относительно предыдущего шага. Возможны и другие подходы.

4. Разработать модели формирования информационных вандалов, криминальных элементов, террористов и модели угроз населению через современные каналы информационного воздействия. Получение первых моделей предусматривает формализацию среды их порождения, мотиваций при принятии асимметричных решений. Создание вторых моделей включает формализацию типовых способов деструктивных воздействий на объекты защиты, исследование само- и не воспроизводящихся, психологически, биологически и социально опасных информационных воздействий на население, прежде всего, через средства массовой информации.

Для моделирования этих процессов могут быть использованы методы искусственного интеллекта [29–32], теории вероятностей, автоматные подходы и другие. Для синтеза и анализа самовоспроизводящихся структур применимы методы, предложенные в [10, 28].

Труды СПИИРАН. 2009. Вып. 8. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2009. Issue 8. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

5. Развить теорию мониторинга информационных угроз населению со стороны ИВ, ИК, ИТ, методы оперативного их вскрытия и прогнозирования. Это развитие предполагает совершенствование методов наблюдения за потенциально опасными каналами деструктивных информационных воздействий и контроля безопасности имеемых информационных ресурсов. Нужны новые, более совершенные, методы распознавания статичных и динамичных информационных угроз, оценки достоверности информации, прогнозирования развития анализируемых процессов.

При таком развитии следует принять во внимание результаты работ [10, 29, 37–39] и других.

6. Разработать методы оперативного синтеза и реализации целесообразных мероприятий противодействия ИВ, ИК, ИТ. Желательно совершенствовать методы автоматического извлечения знаний из наблюдений за процессами ИВ, ИК, ИТ. Требуют дальнейшего развития методы автоматического синтеза структурно-сложных программ противодействия угрозам с учетом возможностей их реализации на практике в приемлемые сроки.

В интересах этого рекомендуется опираться на известные методы интеллектуальной обработки данных [34–36], дедуктивного синтеза программ [28, 30, 33] и другие. Для доказательства существования результативных программ при дедуктивном синтезе на знаниях можно использовать прямой логический вывод, а для извлечения этих программ из вывода – обратный вывод.

7. Разработать принципы построения средств автоматической проверки телевизионных и радиопередач, информации, получаемой через Интернет, цифровых фильмов и музыки, компьютерных игр, газет, журналов, учебной, художественной и технической литературы по требованиям безопасности для населения. Необходимы поиск методов обоснования современных требований к характеристикам, составу и структуре этих средств, а также разработка универсальных технологий их построения с обеспечением защиты от программных деструктивных воздействий.

Разработка этих принципов должна базироваться на результатах решения предыдущих проблем и общих современных подходах к построению программных и аппаратных средств.

8. Совершенствовать теорию построения глобальных систем защиты населения от информационного вандализма и терроризма. Следует совершенствовать нормативную основу такой защиты, разработать международные требования к информации глобального распро-

Труды СПИИРАН. 2009. Вып. 8. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2009. Issue 8. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

странения по безопасности. Необходимо развить методы синтеза и анализа таких систем, управления информационной безопасностью на различных уровнях иерархии общества.

При решении этой проблемы, наряду с вышеизложенными положениями, требуется учет современных подходов к анализу и синтезу структурно сложных организационно-технических систем.

4. Возможные практические пути решения сформулированных проблем и ожидаемые результаты. Решение сформулированных проблем возможно только при объединении ученых различных областей знаний, формирования специальной государственной целевой программы на проведение этих исследований и разработок. Все возможности у Российской Федерации для этого есть, необходима, прежде всего, интеграция и координация усилий ведущих институтов страны со стороны Российской академии наук и, несомненно, финансовая поддержка этих работ. В результате могут быть получены инновационные результаты, позволяющие существенно снизить риски от ИВ, ИК, ИТ, повысит информационную безопасность Российской Федерации.

На основе этих результатов, наряду с запретительными мерами, может быть широко реализован рекомендательный подход при предоставлении различного рода информации населению. Суть этого подхода в том, чтобы при предоставлении населению информации, прежде всего через средства массовой информации и Интернет, шло сопровождение ее рекомендациями по безопасности применения. Несомненно, вручную (старыми методами) выработка таких рекомендаций в современных условиях практически не реальна. Для этого нужны специальные методы и средства автоматической оперативной проверки информации по основным требованиям безопасности и генерации рекомендаций населению. Получив такие рекомендации человек сам должен принимать решение использовать эту информацию или нет. При таком подходе не нарушаются конституционные права граждан на информацию, не ограничивается свобода слова, в то же время существенно снижаются риски деструктивных информационных воздействий на население.

Заметим, что оперативная проверка информации по требованиям безопасности позволит выявлять не только деструктивные, но и позитивные воздействия на людей, превратить информацию в эффективное «лекарство».

Планируемые результаты также могут дать возможность:

Труды СПИИРАН. 2009. Вып. 8. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2009. Issue 8. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

- количественно обосновывать системные решения, принимаемые на различных уровнях государственного и военного управления, как по вопросам внутренней, так и внешней информационной безопасности;
- своевременно прогнозировать и предотвращать возможные информационные «катаклизмы» в обществе.

В целом они позволят:

- совершенствовать существующую систему информационной безопасности Российской Федерации;
- устранить имеющиеся перекосы, сосредоточить внимание на ключевых позициях, снизить необоснованные затраты на решение проблем информационной безопасности;
- стимулировать гармоничное, сбалансированное развитие экономики и самого общества за счет совершенствования управления современным информационным потоком.

Литература

1. *Цыгичко В.Н., Смолян Г.Л., Черешкин Д.С.* Информационное оружие как геополитический фактор и инструмент силовой политики. М.: Институт системного анализа РАН, 1997. 37 с.
2. *Расторгуев С.П.* Информационная война. М.: Радио и связь, 1998. 415 с.
3. *Прокофьев В.Ф.* Тайное оружие информационной войны: атака на подсознание.2-е изд. М.: СИНТЕГ, 2003. 408 с.
4. *Астахов М.А., Ростовцев Ю.Г., Яфраков М.Ф.* Информационная борьба. М.: Издательство «ТОМ», 2007. 334 с.
5. *Бухарин С.Н., Цыганов В.В.* Методы и технологии информационных войн. М.: Академический Проект, 2007. 382 с.
6. *Лисичкин В.А., Шелепин Л.А.* Третья мировая (информационно-психологическая) война. 2-е изд. М.: Институт социально-психологических исследований АСН, 2000. 304 с.
7. *Цыганков В.Д.* Психотроника и безопасность России. М.: СИНТЕГ, 2003. 136 с.
8. *Смолян Г.Л., Зараковский Г.М. и др.* Информационно-психологическая безопасность (определение и анализ предметной области). М.: Институт системного анализа РАН, 1997. 52 с.
9. *Цыганов В.В., Бухарин С.Н.* Информационные войны в бизнесе и политике. Теория и методология. М.: Академический Проект, 2007. 336 с.
10. *Осипов В.Ю., Ильин А.П. и др.* Радиоэлектронная борьба. Теоретические основы. Петродворец: ВМИРЭ, 2006. 302 с.
11. *Котенко И.В., Юсупов Р.М.* Информационные технологии для борьбы с терроризмом // Защита информации. ИНСАЙД. 2009. . №2 (26). С. 74–79.
12. Вишняков Я.Д., Бондаренко Г.А. и др. Основы противодействия терроризму. / Под ред. Я.Д.Вишнякова. – М.: Издательский центр «Академия», 2006. 240 с.
13. *Афонин С.А. и др.* Современный терроризм и борьба с ним: социально – гуманитарные измерения. / Под ред. В.В.Ященко. М.: МЦНМО, 2007. 216 с.

Труды СПИИРАН. 2009. Вып. 8. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2009. Issue 8. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

14. *Андреев О.О.* и др. Критически важные объекты и кибертерроризм. Часть 1, 2. / Под ред. В.А.Васенина. М.: МЦНМО, 2008. 398 с (часть 1), 607 с (часть 2).
15. *Фролов Д.Б.* Информационная геополитика и вопросы информационной безопасности. // Национальная безопасность. 2009. № 1. С. 72–79
16. *Пирумов В.С.* Стратегия выживания социума. Системный подход в исследовании проблем геополитики и безопасности. М.: Дружба народов, 2003. 544 с.
17. Доктрина информационной безопасности Российской Федерации. Утверждена Президентом Российской Федерации 9 сентября 2000 года.
18. *Астахов М.А., Ростовцев Ю.Г., Яфраков М.Ф.* Информационная борьба и знаковые системы. М.: Издательство «ТОМ», 2007. 334 с.
19. *Юсупов Р.М.* Наука и национальная безопасность. СПб.: Наука, 2006. 455 с.
20. 2007 Report on Terrorism. USA. National Counterterrorism Center. 2008. 30 April. 96 p.
21. *Иванов М.Н., Васильчинко А.В., Юсупов Р.Ф.* Склонность к терроризму: психофизиологический, этнический анализ (стратегии управления и мониторинга групп риска в этническом регионе) // Взаимопонимание культур, проблемы национальных идентичности (к 125-летию М. Гафури): Сборник научных статей. Уфа: 2009. С. 148–153.
22. *Ильясов Ф.Н.* Терроризм - от социальных оснований до поведения жертв. Социологические исследования. 2007. № 6. С. 78–85.
23. *Жаринов К. В.* Терроризм и террористы**:** Ист. справочник / Под общ. ред. А. Е. Тараса. Мн.: Харвест, 1999. 606 с.
24. *Osipov V., Ivakin Y.* Terrorists: Statistical Profile / Information Fusion and Geographic Information Systems. Proceedings of the Fourth International Workshop, 17–20 May 2009. Springer-Verlag Berlin Heidelberg 2009. pp. 241–250.
25. *Peter Hancock.* The Human Factors Response to Terrorism. COMMITTEE ON HUMAN FACTORS. Washington, D.C., December 5–7, 2001. Fifty-fourth Meeting. По состоянию на 24.06.2009 доступно на веб-сайте http://www.apa.org.
26. *Sandra G. Hart.* Human Factors and Aviation Security. COMMITTEE ON HUMAN FACTORS. Washington, D.C., December 5-7, 2001. Fifty-fourth Meeting. По состоянию на 24.06.2009 доступно на веб-сайте http://www.apa.orgmtemeet.
27. Технические методы и средства защиты информации / Ю.Н.Максимов, В.Г.Сонников, В.Г.Петров и др. СПб.: ООО «Издательство Полигон», 2000. 320 с.
28. *Осипов В.Ю.* Информационная безопасность: синтез управляющих программ. Петродворец: ВМИРЭ, 2001. 64 с.
29. *Поспелов Д.А.* Ситуационное управление: теория и практика. М.: Наука, 1986. 288 с.
30. Искусственный интеллект. В 3-х кн. Кн. 2 Модели и методы: Справочник / Под ред. Д.А.Поспелова. М.: Радио и связь, 1990. 304 с.
31. *Рассел С., Норвиг П.* Искусственный интеллект: современный подход, 2-е изд.: Пер. с англ. М.: Издательский дом «Вильямс», 2006. 1408 с.
32. *Хайкин С.* Нейронные сети: полный курс, 2-е изд. Пер. с англ. М.: Издательский дом «Вильямс», 2006. 1104 с.
33. *Осипов В.Ю.* Синтез результативных программ управления информационно-вычислительными ресурсами // Приборы и системы управления. 1998. № 12. С. 24-27.
34. *Городецкий В., Самойлов В., Малов А.* Технология обработки данных для извлечения знаний: Обзор состояния исследований. Новости искусственного интеллекта. 2002. № № 3-4.

Труды СПИИРАН. 2009. Вып. 8. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2009. Issue 8. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

35. *Jiawei Han, Micheline Kamber.* Data Mining: Concepts and Techniques, 2nd ed. The Morgan Kaufmann Series in Data Management Systems, Jim Gray, Series Editor Morgan Kaufmann Publishers, March 2006. ISBN 1-55860-901-6.
36. *Багдесян А.А., Куприянов М.С., Степаненко В.В.* Технологии анализа данных: Data Mining, Visual Mining, Text Mining, OLAP, 2-е изд. СПб.: BHV, 2007. 384 с.
37. *Городецкий В., Карсаев О., Самойлов В.* Многоагентная система оценки ситуаций на основе асинхронного потока распределенных гетерогенных данных. Труды Международной конференции "Искусственные интеллектуальные системы", Дивноморское, Россия, сентябрь 3-9, Физматгиз, 2004. с.294-300.
38. *Кулешов С.В.* Аналитический мониторинг Интернет ресурсов с целью выявления потенциально опасного содержания. // Материалы четвертой научно-практической конференции «Перспективные системы и задачи управления». Таганрог, 2009. С. 255.
39. *Александров В.В., Кулешов С.В.* Аналитический мониторинг INTERNET контента. Инфологический подход // Системные проблемы надежности, качества, математического моделирования, информационных и электронных технологий в инновационных проектах (Инноватика – 2007). // Материалы Международной конференции и Российской научной школы. Часть 2, Том 1. М.: Энергоатомиздат, 2007. С. 80–83.

Осипов Василий Юрьевич — д.т.н., проф.; ведущий научный сотрудник Санкт-Петербургского института информатики и автоматизации РАН (СПИИРАН). Область научных интересов: информационное противоборство, моделирование, искусственный интеллект. Число научных публикаций — 96. osipov_vasiliy@mail.ru; СПИИРАН, 14-я линия ВО, д. 39, Санкт-Петербург, 199178, РФ; р.т. 8 (812) 328-01-79.

Osipov Vasily Yurevich — Dr.Sci.Tech., the professor; the leading scientific employee of the St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences (SPIIRAS). Research interests: information antagonism, modelling, artificial intelligence. The number of publications — 96. osipov_vasiliy@mail.ru; SPIIRAS, 39, 14-th Line V.O., St. Petersburg, 199178, Russia; office phone 8 (812) 328-01-79.

Юсупов Рафаэль Мидхатович — член-корреспондент РАН, Заслуженный деятель науки и техники РФ, д.т.н., проф., директор Санкт-Петербургского института информатики и автоматизации РАН (СПИИРАН). Область научных интересов: информатика, моделирование, теория управления (теория адаптивных систем, идентификация, теория чувствительности), информатизация общества и информационная безопасность. Число публикаций — более 350. yusupov@iias.spb.su; СПИИРАН, 14-я линия ВО, д. 39, Санкт-Петербург, 199178, РФ; р.т. 8 (812)328-33-11, (812)328-34-11, факс: 8 (812)328-4450.

Yusupov Rafael Midhatovich — Corresponding member of the Russian Academy of Science, the Honored worker of a science and technics of the Russian Federation, Dr.Sci.Tech., the professor, director of the St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences (SPIIRAS). Research interests: computer science, modelling, the theory of management (the theory of adaptive systems, identification, the theory of sensitivity), information of a society and information safety. The number of publications — More than 350. yusupov@iias.spb.su; SPIIRAS, 39, 14-th Line V.O., St. Petersburg, 199178, Russia; office phone 8 (812) 328-33-11, 8 (812) 328-34-11, fax 8 (812)328-4450.

Труды СПИИРАН. 2009. Вып. 8. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2009. Issue 8. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru