Раздел I. Комплексная защита объектов информатизации

УДК 681.324 + 159.9

Д.А. Астахов

РЕШЕНИЕ ПРОБЛЕМЫ СДЕРЖИВАНИЯ ГОНКИ ИНФОРМАЦИОННЫХ ВООРУЖЕНИЙ НА ОСНОВЕ ПСИХОЛОГИИ РИСКОВ

Раскрыты понятия информационного оружия, информационной войны. Прослежена история международной правовой базы по вопросам информационного оружия, развития информационной сферы. Проанализированы причины недооценки угроз информационного оружия для международных отношений и сохранения мира. Выведены рекомендации для улучшения грамотности населения по вопросам информационного вооружения и информационно-психологической безопасности.

Информационное оружие; информационная война; гонка информационных вооружений; информационно-психологическая безопасность; психология рисков; международные отношения.

D.A. Astakhov

INFORMATION ARMS RACE INHIBITION PROBLEM'S SOLUTION IN TERMS OF RISK PSYCHOLOGY

In the article these are discovered terms of information weapon, information war. It is retraced international legal system for information weapons and development of information area. It is examined the reasons underestimation of information weapon's threats for international relationship and preservation of peace. There are some recommendations for improvement of people's literacy on the matter of information weapons and information-psychological security.

Information weapon; information war; information armaments drive; information-psychological security; risk psychology; international relationship.

С переходом от индустриального общества к информационному и развитием информационных технологий значительное внимание уделяется новейшим видам так называемого “гуманного оружия”. К ним относятся информационное, психотронное, экономическое, консциентальное оружие и пр. Особое место среди них занимает информационное оружие и технологии ведения информационной войны. Информационным оружием называются способы и средства информационного воздействия на технику и людей с целью решения задач воздействующей стороны [5].

Универсальность, скрытность, многовариантность форм реализации, радикальность воздействия, достаточный выбор времени и места применения и, наконец, экономичность делают информационное оружие чрезвычайно опасным. Оно легко маскируется под средства защиты, например, интеллектуальной собственности; позволяет вести наступательные действия анонимно, без объявления войны.

Увеличение воздействия на индивидуальное и общественное сознание за счет новейших информационных технологий и средств, причем, в первую очередь, – со стороны высокоразвитых стран, ведет к изменению глобального и регионального балансов сил, внесению дополнительной напряженности между традиционными и нарождающимися центрами силы, появлению новых сфер конфронтации. Правомерно утверждать: чем большими возможностями в информационной сфере обладает государство, тем легче оно может добиться геополитических стратегических преимуществ [1].

Михаил Делягин, директор Института проблем глобализации, утверждает, что для обществ со «слабой демократией» информационные войны носят абсолютно разрушительный характер, являясь своего рода оружием массового уничтожения, которое поражает не только противника, против которого было направлено, но и всю окружающую среду, в данном случае – социум, заражая его истеричностью и тотальным недоверием, которое парализует и экономический прогресс [2].

По некоторым данным, в той или иной степени разработки таких средств ведутся в 120 странах. Для сравнения: разработки в области ядерного оружия ведутся не более чем в 20 странах. Ведется, а в некоторых странах уже завершена разработка средств информационного противоборства с вероятными противниками как в условиях военных конфликтов различной степени интенсивности, так и в мирное время, причем не только на стратегическом, но и на оперативном и даже тактическом, вплоть до поля боя, уровнях. Большое внимание уделяется вопросам защиты собственного информационного пространства от действия информационного оружия со стороны враждебных государств, несанкционированного воздействия на инфосферу.

По мнению политологов, развитие информационных технологий уже сейчас ведет к кардинальному изменению самого способа ведения войн и облика вооруженных сил. Неслучайно в бюджетах некоторых ведущих стран расходы на информационную безопасность предусматриваются в одном пакете с ассигнованиями на защиту от применения оружия массового уничтожения. Массовые армии в будущем уступят место относительно небольшим по численности вооруженным силам, укомплектованным исключительно профессионалами – специалистами по информационному противоборству. США создали информационные войска и выпускают подразделения кибервоинов. Сегодня в директивах Министерства обороны США подробно излагается порядок подготовки к информационным войнам. Пентагон на суперкомпьютерах моделирует варианты возможных войн в XXI столетии с использованием методов и технологии “несмертельного оружия”.

В условиях масштабности, жизненно важной значимости и одновременно уязвимости складывающейся глобальной информационной структуры применение информационного оружия как средства ведения широкомасштабных войн может вызвать последствия, вполне сравнимые по силе своего воздействия на критически важные структуры с “традиционным” оружием массового уничтожения (ОМУ). Но война с применением информационного оружия в отличие от “классических” видов ОМУ может носить и внутренний характер. Это оружие как нельзя лучше подходит для применения в гражданских целях, в борьбе за власть, в сепаратистских и

межнациональных конфликтах, а также в террористических и криминальных целях.

Страны, не способные пока создать собственные средства информационного воздействия, начинают проявлять интерес к закупкам таких средств у стран, становящихся тем самым пролиферантами новых видов вооружений. К этому процессу уже подключились политические группировки, “новый” оружейный бизнес, а наряду с ними – террористические и криминальные организации и группы.

Особое внимание необходимо уделить одной из форм информационного оружия – консциентальному оружию, где предметом поражения и уничтожения являются определенные типы сознаний. В результате консциентальной войны определенные типы сознаний должны быть уничтожены, перестать существовать, их не должно быть. А носители этих сознаний, наоборот, могут быть сохранены, если они откажутся от собственных форм сознания – предметов разрушения и поражения.

Прежде всего, этот тип воздействий по смене и преобразованию типов имиджидентификаций (глубинного отождествления с той или иной позицией, представленной конкретным образом) и аутентизаций (чувства личной подлинности) осуществляют средства массовой информации, и, прежде всего, телевидение.

Поражение СССР в холодной войне связано с использованием консциентального оружия, развал СССР – это тоже результат его использования. И с помощью этих же средств происходят сегодня все основные действия по разрушению сознания российского народа.

Основная цель консциентальной войны: диаспоризация российского народа, фрагментация региональных и социально-стратовых общностей на основе слома всех существующих имиджидентификаций. Конечная цель использования консциентального оружия – это изымание людей из сложившихся форм мегаобщностей. Разрушение народа и превращение его в население происходит за счет того, что никто больше не хочет связывать и соотносить себя с тем полиэтносом, к которому до этого принадлежал. Разрушение сложившихся имиджиндентификаций нацелено на разрушение механизмов включения человека в естественно сложившиеся и существующие общности и замена этих эволюционно-естественно сложившихся общностей одной полностью искусственной – общностью зрителей вокруг телевизора. Неважно, как человек при этом относится к тому, что он видит и слышит с экрана телевизора, важно, чтобы он был постоянным телезрителем, поскольку в этом случае на него можно направленно и устойчиво воздействовать [4]. Следовательно, прогресс в информационных технологиях так же, как ранее в ядерных, чреват новым витком гонки вооружений, который вновь отвлечет огромные ресурсы от целей мирного созидания.

Из этого следует, что по опасности угроз и социальных последствий мы можем поставить ядерное и информационное оружие на одну ступень. И ядерное, и информационное оружие – это оружие двойного назначения. С одной стороны, мы знаем о сравнительно дешёвой энергии атома, что составляет основу атомной энергетики. Процесс информатизации также имеет много положительных сторон: доступность и многообразность информации, с помощью которой человек более эффективно осуществляет профессиональную деятельность, становится свободнее, увереннее, функционально-грамотнее и т.д.

С другой стороны, информация и атомная энергия могут иметь для человека негативный эффект – создание новых видов оружия. Ядерное оружие впервые встало на вооружение в армии США в 1945 году. В августе того же года оно было впервые использовано в боевых условиях против японских городов Хиросима

(6 августа) и Нагасаки (9 августа), что стало нечто вроде апогея в этой сфере – оно прошло испытание на людях. Человечество осознало, увидело своими глазами чудовищные последствия таких разработок. В 1949 году ядерное оружие появилось у СССР, так началась «ядерная гонка». Ядерное оружие стало неотъемлемым инструментом дипломатии обеих стран.

Позже появились инициативы по сокращению смертоносного оружия. Ядерное разоружение – процесс сокращения арсеналов ядерного оружия, его носителей и средств доставки, а также производства, что позволит снизить шанс возникновения ядерной войны.

Началом разоружения принято считать Карибский кризис 1962 года, когда мир впервые оказался на грани ядерной катастрофы. Причиной тому послужило размещение американских ракет средней дальности в Турции, спровоцировавшее Советский Союз на экстренную установку аналогичных ракет на Кубе. Одним из последствий Карибского кризиса стало возникновение на Западе мощного общественного движения в поддержку ядерного разоружения. С тех пор подписано множество документов, регламентирующих разработку ядерного оружия. Такие документы постоянно разрабатываются и принимаются и в наши дни. В этом направлении активно работают такие организации как ООН, Совет Европы, ЮНЕСКО и др.

Другая ситуация наблюдается в сфере производства информационного оружия и информационного разоружения. Данный вид оружия невидим, неосязаем, анонимен, скрытен, уличить кого-либо в его использовании очень сложно. Если об испытании ядерного оружия мгновенно узнает весь мир, всех это потрясает и шокирует, то информационное оружие невидимо применяется каждый день, но человек этого может не замечать, не чувствовать, становясь его жертвой.

Информационное оружие опасно так же, как и ядерное. Поэтому необходимо регулирование информационной сферы и сферы информационного вооружения. По мнению Ю. А. Полякова, запретить разработку и использование информационного оружия невозможно. Ограничить усилия многих стран по формированию единого глобального информационного пространства также нереально. Однако Россия может выступать инициатором заключения разумных соглашений, опирающихся на международное право и минимизирующих угрозу применения информационного оружия [4].

Так, на основе российского проекта 4 декабря 1998 года консенсусом была принята Резолюция 53-й сессии ГА ООН 53/70 "Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности", хотя и в “смягченном” виде. Из проекта исчезли многие конкретные предложения по организации практического противодействия возможному военному применению информационных технологий, констатации опасности создания информационного оружия и разжигания информационных войн. Но вместе с тем на уровне ООН впервые международным сообществом единодушно было признано наличие военной составляющей мирового процесса информатизации. Это явилось важным политическим достижением.

На 54-й сессии Генеральной Ассамблеи Организации Объединенных Наций в числе документов, имеющих глубокие и далеко идущие политические последствия для дипломатии и стратегической стабильности XXI века, была принята резолюция 54/49 “Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности” (1999). Мировое сообщество признало международную информационную безопасность уже как глобальную проблему, как необходимое условие существования человеческого сообщества в послеядерный век.

Именно в этом – основной итог принятия 54-й сессией Генассамблеи 1 декабря 1999 года резолюции 54/49.

Примерно с начала 90-х годов вопрос информационного оружия и информационных войн стал довольно широко обсуждаться специалистами, появилось большое число публикаций, на многих конференциях, семинарах, симпозиумах в том или ином виде поднимались вопросы немирного использования программно-технических разработок и путей защиты информационного ресурса от их воздействия. Однако все эти обсуждения и публикации были далеки от международно-переговорного круга проблем и не вызывали большого интереса у неспециалистов. В этом отношении принятие названных резолюций послужило предупредительным знаком об существовании опасности. Оказалось, что к этому времени уже имелись не только значительные наработки в области создания средств воздействия на информационный ресурс, но и многочисленные факты неоспоримо военного применения средств, которые иначе как информационным оружием названы быть не могут [3,6].

Кроме резолюций ГА ООН, существуют и рекомендации Европейской комиссии по построению информационного общества, представленные как основные задачи информационной политики развитых стран: совершенствование и развитие информационно-телекоммуникационной инфраструктуры; обеспечение широкого, свободного доступа к информационным ресурсам; обеспечение граждан и общества значимой и востребованной информацией; подготовка человека к жизни и работе в информационном обществе. В Конвенции по киберпреступности, одобренной в последние годы Советом Европы, основными направлениями международного сотрудничества в области обеспечения информационной безопасности определены: запрещение разработки, распространения и применения информационного оружия; обеспечение безопасности международного информационного обмена, в том числе сохранности информации при ее передаче по национальным телекоммуникационным каналам и каналам связи; координация деятельности правоохранительных органов стран, входящих в мировое сообщество, по предотвращению компьютерных преступлений; предотвращение несанкционированного доступа к конфиденциальной информации в международных банковских телекоммуникационных сетях и системах информационного обеспечения мировой торговли, к информации международных правоохранительных организаций, ведущих борьбу с транснациональной организованной преступностью, международным терроризмом, распространением наркотиков и психотропных веществ.

В активе Совета Европы около 100 проведенных с 1968 г. конференций, коллоквиумов и совещаний, посвященных информационным проблемам на континенте. И почти на всех из них при обсуждении актуальных вопросов затрагивались проблемы информационной безопасности.

Очевидно, что до сих пор не решены многие проблемы деятельности средств информации и коммуникации на международной арене, а это является причиной возникновения различных конфликтов и разногласий между государствами, обострения международной обстановки. Такое положение дел ведет к созданию взрывоопасных ситуаций, угрожающих миру и международной безопасности.

Анализ, предпринятый в нашем исследовании, показал, что главной причиной недооценки проблемы информационного разоружения в рамках международного права являются специфические свойства информационного оружия: скрытость, анонимность, массовость, минимальные затраты, возможность избежать человеческих потерь и др.

Еще одна причина выявлена нами при использовании нового научного направления – психологии безопасности.

Современному человеку, который каждый день оказывается объектом информационного воздействия различных сил, надо понимать вопросы, касающиеся информационной сферы, технологий, оружия, чтобы уметь противостоять угрозам. Очень важно для него осознавать, когда он находится в опасности и безопасности и отличать её степень.

Брюс Шнайер, известный американский криптограф, в своей статье «Психология безопасности» говорит о том, что существуют дисциплины, которые изучают чувство безопасности: откуда оно появляется, как оно проявляется, и достаточно подробно объясняют различия между ощущением и реальностью безопасности и, что более важно, из чего эти различия проистекают:

1) поведенческая экономика, иногда называемая поведенческим финансированием, рассматривающая человеческие факторы – эмоциональные, социальные и познавательные – и то, как они влияют на принятие экономических решений;

2) психология принятия решений (теория ограниченной рациональности), которая изучает, как мы принимаем решения и рассматривает риски, связанные с безопасностью;

3) прямое исследование психологии риска. Психологи изучают восприятие риска, пытаясь выяснить, когда мы преувеличиваем опасность рисков и когда придаем ей меньшее, чем следовало бы, значение;

4) неврология. Психология безопасности очень тесно связана с тем, как мы думаем, причем принимаются во внимание как интеллектуальный, так и эмоциональный аспекты.

Б. Шнайер обосновывает, что безопасность – это компромисс. Мы идем на компромиссы ради безопасности каждый день. Большую часть времени мы даже не осознаем этого, так как мы идем на них интуитивно. Однако человек преувеличивает одни риски, тогда как преуменьшает значение других.

Существует несколько определенных аспектов, которые могут быть оценены неверно при принятии компромиссных решений в области безопасности: степень серьезности риска; вероятность риска; объем затрат; эффективность контрмер, снижающих вероятность риска; возможность адекватного сопоставления рисков и затрат.

Чем больше у человека ощущение этих аспектов расходится с реальностью, тем меньше его воображаемый компромисс будет соответствовать действительности. Если он считает, что риск гораздо серьезнее, чем это есть на самом деле, то на уменьшение риска он затратит больше, чем нужно. Если по какой-либо причине думать, что риск существует, но он касается только других людей, затраты будут недостаточными. Если переоценить стоимость контрмер, то вероятность применить их в нужное время невелика, а если переоценить эффективность контрмер, есть вероятность применить их тогда, когда в этом нет необходимости. Если неточно определить суть компромисса, то невозможно правильно сбалансировать затраты и эффективность контрмер.

Брюс Шнайер отмечает ряд основных ошибок:

- люди преувеличивают производящие сильное впечатление риски и преуменьшают значение обычных;
- у людей возникают проблемы в оценке рисков во всем, что выходит за рамки обычного положения вещей;
- персонифицированные риски считаются более опасными, чем анонимные;

- люди недооценивают риски, на которые идут самостоятельно, и переоценивают те, которые не могут контролировать;
- и, наконец, люди переоценивают риски, которые у всех на слуху и являются объектом общественного внимания.

Автор приводит также общепринятые взгляды на восприятие риска людьми (табл. 1).

Таблица 1

Общепринятые взгляды на восприятие риска людьми

Люди преувеличивают риски, которые:	Люди преуменьшают значение рисков, которые:
Производят глубокое впечатление	Не привлекают внимание
Случаются редко	Являются обычными
Персонифицированы	Анонимны
Обсуждаются	Не обсуждаются
Преднамеренные или спровоцированные человеком	Естественные
Угрожают непосредственно	Угрожают в будущем или границы которых размыты
Внезапны	Развиваются медленно, со временем
Угрожают человеку лично	Угрожают другим

Природные способности защиты от угроз могут намеренно блокироваться другими людьми – политиками, маркетологами и так далее – то есть теми, кто эксплуатирует в своих целях сбои наших естественных способностей.

Б. Шнайер вводит понятие «эвристика аффекта» (автоматическая оценка, сделанная в состоянии аффекта), которая заключается в том, что положительная эмоциональная оценка ситуации ведет к притуплению восприятия риска, а отрицательная оценка ведет к обострению восприятия риска. Это объясняет, почему люди склонны недооценивать риски, которые подразумевают некоторую выгоду (курение, опасные виды спорта и так далее), но также имеют негативные эффекты.

Людей убеждает более яркая, личная история, а не голая статистика и факты. Теперь, когда мы получаем информацию с помощью телевидения, газет и Интернета, ситуация изменилась. То, о чем мы читаем, то, что кажется нам ярким, – скорее всего очень редкое и зрелищное явление. Это может быть и чем-то выдуманным, как например, кино или телевизионное шоу. Это может быть информация маркетингового характера – коммерческая или политическая. При этом следует помнить, что визуально демонстрируемый материал воспринимается острее, чем информация в печатных средствах массовой информации. Этим объясняется, почему мы обеспокоены угрозами, о которых сообщается в новостях, а не теми, о которых в них не рассказывают, или почему мы обеспокоены редкими угрозами, о которых узнали из эмоционально рассказанных личных историй, а не угрозами столь обычными, что они представлены лишь сухими статистическими данными [7].

Положения психологии рисков объясняют и проблему информационного разоружения. Если проблемы ядерного оружия известны уже достаточно давно, они активно освещаются в СМИ, о них много говорят на высшем уровне, то об информационном оружии люди информированы плохо, его воздействия постоянны и анонимны. Исходя из психологии рисков, жители планеты должны больше бояться

ядерного оружия, недооценивая угрозу информационного оружия как ОМУ. Тем самым степень неосведомлённости человека о негативных информационных воздействиях, которые направлены на него ежеминутно, высока. Поэтому стремительно возрастает степень риска. СМИ – источник информации, которому доверяют, а заметить использование информационного оружия телевидением, радио и прессой невозможно.

Люди преуменьшают значение риска информационного оружия, потому что оно не привлекает внимания и является чем-то обыденным. Человек, не задумываясь, смотрит телепередачи или новости каждый день, подвергаясь определённому программированию. Анонимность воздействия также способствует его скрытости, поэтому его не обсуждают, поэтому сфера действия информационного оружия расширяется незаметно. Если даже человек когда-нибудь и слышит о таком понятии, как информационное оружие, то он не признаёт в нём опасности для себя. Сам являясь его объектом, он думает, что это является опасностью для других. Большинство людей недостаточно информированы об этом, поэтому пребывают в заблуждении в отношении информационного оружия.

Для решения проблемы сдерживания гонки информационных вооружений необходимы интенсивные и решительные шаги мировой общественности. Шаги, предпринятые для ядерного разоружения, должны реализовываться и для информационного разоружения. Так, Ю.А. Поляков остро ставит вопрос о разработке основ международной информационной безопасности:

1) сотрудничество в свободном и беспрепятственном распространении идей мира, разоружения, взаимопонимания, международной безопасности с помощью СМИ;

2) безусловное уважение в международной практике права каждого народа суверенно избирать формы и пути своего информационного развития;

3) исключение из международной практики всех форм информационной дискриминации;

4) отказ от политики информационного диктата;

5) установление гарантии на равную информационную безопасность всех государств;

6) ликвидация на правовых основах внутренних и внешних барьеров, препятствующих свободному обмену и более широкому и сбалансированному распространению информации и различных точек зрения;

7) взаимное уважение свободы печати и информации;

8) содействие развитию всех видов информационной деятельности на благо и в интересах экономического и социального развития народов.

Международная информационная безопасность должна быть всеобъемлющей. Становление и развитие мировой информационной индустрии объективно влияет на усиление взаимосвязи и взаимозависимости разных регионов и стран современного мира и вызывает необходимость решения большого числа международно-правовых проблем, связанных с осуществлением информационной деятельности на международной арене. Отсутствие четких политико-правовых решений в этой области человеческой деятельности прямо ведет к возникновению негативных явлений в международной жизни, обострению отношений между государствами и народами. Устранить причины конфликтов в сфере международных информационных связей можно, только создав крепкий юридический фундамент международных информационных отношений. Для этого Ю.А.Поляков формулирует необходимые для разработки основные принципы международного информационного права: уважения суверенной информационной свободы, информацион-

ного невмешательства, равенства, сотрудничества; информационной справедливости, гуманизма, содействия информационному развитию народов; уважения основных прав и свобод человека при распространении информации, а также содействия использованию информационных ресурсов в соответствии с международным правом, содействия в распространении информации в целях укрепления доверия и взаимопонимания между народами; информационной ответственности.

Разработка и принятие этих принципов могли бы серьезно укрепить мировой информационный порядок, активизировать сотрудничество между государствами по вопросам информации, а также стимулировать решение специальных вопросов информационной деятельности. Эти принципы могли бы также образовать юридическое ядро международного информационного права, что положило бы начало самостоятельному существованию новой отрасли международного права [4].

Всё больше документов должно приниматься на уровне не только международных организаций, таких как ООН и ЮНЕСКО, но и на федеральном и региональном уровне Российской Федерации. Федеральный закон РФ «Об информационно-психологической безопасности», проект которого давно обсуждается, должен быть принят в кратчайшие сроки.

Считаем, что предотвращение воздействия информационного оружия на Россию как суверенное государство должно стать приоритетной задачей соответствующих структур и должностных лиц. В соответствии с упомянутой в работе психологией риска необходимо выработать как национальные, так и региональные стратегии противодействия негативным информационным воздействиям. Для адекватного восприятия действительности и взвешенной оценки угроз люди должны быть хорошо информированы о предмете риска, в нашем случае – об информационном оружии. После бомбардировки Хиросимы–Нагасаки о ядерном оружии заговорили на всей планете. Но весьма сомнительно ждать такого события с участием информационного оружия, наоборот нужно всеми силами и средствами предотвратить подобное. Поэтому говорить об информационном оружии, его субъектах и объектах надо чётко, понятно и много. Это поможет развеять миф о том, что информационное оружие «угрожает другим», а не человеку, который воспринимает эту информацию. Также следует донести до людей информацию о том, кто и как пытается воздействовать и трансформировать их сознание, чтобы нейтрализовать такое свойство информационного оружия, как анонимность. Иными словами, привлечь внимание общественности к вопросам информационного оружия – такая цель должна преследоваться мировым сообществом в XXI веке. Все инициативы по регулированию информационной сферы должны закрепляться нормативными актами, а главное – реализовываться на практике. На международном уровне по данному вопросу должна продолжать работу ООН. В России на федеральном уровне ответственность за информирование населения может нести Национальный антитеррористический комитет, а на региональном уровне – Антитеррористические комиссии, в обязанности которых может входить координирование работы субъектов информирования об информационном оружии и информационно-психологической безопасности личности. Субъектами такой деятельности могут быть, во-первых, СМИ как популяризатор знаний об опасностях информационного оружия и необходимости защиты от него. Во-вторых, информирование должно затронуть систему высшего образования. Со студентами вузов должны регулярно проводиться беседы и занятия, раскрывающие сущность и глубину вопросов об информационном вооружении и способах защиты. В-третьих, аналогичная работа должна вестись на предприятиях, а также в органах государственного управления. Учитывая психологический характер воздействий информационного оружия, а

также достижения психологии рисков, к работе должны привлекаться психологи. Все эти меры повысят грамотность нашего народа в области информационного оружия, а потому будут способствовать повышению уровня национальной безопасности России.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Гриняев С.Н.* Интеллектуальное противодействие информационному оружию. – М., 1999. – С. 5 – 6.

2. *Делягин М.* Информационные войны как оружие массового уничтожения [Электронный ресурс]. – Режим доступа:http://www.rosbalt.ru/2001/11/02/24094.html – Загл. с экрана. – Яз.рус., 09.10.2009.

3. *Крутских А.В., Федоров А.В.* О международной информационной безопасности // Международная жизнь. – 2000. – № 2. – С. 2 – 4.

4. *Поляков Ю. А.* Информационная безопасность и средства массовой информации: Учебное пособие. – М.: ИМПЭ им. А. С. Грибоедова, 2004. – С. 35 – 40.

5. *Прокофьев В.Ф.* Тайное оружие информационной войны: атака на подсознание. – 2-е изд., расшир. и дораб. – М.: СИНТЕГ, 2003. – С. 15 – 18.

6. *Федоров А.В.* Информационная безопасность в мировом политическом процессе: Учеб.пособие. / А.В.Федоров; Моск.гос.ин-т межд.отношений (ун-т) МИД России. – М.: МГИМО-Университет, 2006. – С. 163 – 166.

7. *Шнайер Б.* Психология безопасности, часть вторая. [Электронный ресурс]. – Режим доступа: www.securitylab.ru/analytics/350909.php - Загл.с экрана. – Яз.рус. – 12.10.2009.

Астахов Дмитрий Александрович
Южно-Уральский государственный университет.
E-mail: ada97@yandex.ru.
454080, г. Челябинск, ул. Энгельса, 36А, кв. 16.
Тел.: 8 (351) 265-68-01; 8 (351) 264-08-54.
Кафедра информационной безопасности; студент.

Astakhov Dmitry Alexandrovich
South Ural State University.
E-mail: ada97@yandex.ru.
16 apt., 36A bld., Engelsa str., Chelyabinsk, 454080, Russia.
Phone: 8 (351) 265-68-01; 8 (351) 264-08-54.
The Department of Information Security; student.

УДК 681.586.785

В.В. Браташ, М.А. Каманин

ИНФОРМАЦИОННАЯ СИСТЕМА ДЛЯ МОНИТОРИНГА РАСПРЕДЕЛЕНИЯ ТЕМПЕРАТУРЫ В ПОМЕЩЕНИИ С ПОВЫШЕННОЙ ПОЖАРО- И ВЗРЫВООПАСНОСТЬЮ

Разработка системы из принципиально пожаро- и взрывобезопасных датчиков за счет использования технологии магнитострикционных линий задержки на продольных волнах. В работе приведено описание распределенных по длине датчиков температуры – ферромагнитных волноводов, с помощью которых строится картина распределения по всему помещению и выявляются опасные зоны. Данная