САЦЫЯЛОГІЯ

УДК 316.4

Е.М. Бабосов

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ – ФАКТОР УСТОЙЧИВОГО РАЗВИТИЯ БЕЛАРУСИ

В статье отмечается, что в условиях обострения глобальной нестабильности и конфликта интересов различных стран и их коалиций во втором десятилетии XXI века существенно актуализируется проблематика обеспечения информационной безопасности на евразийском континенте. Под этим углом зрения характеризуются сущность и особенности информационной войны, ее основные формы в современном нестабильном мире. В этом контексте типологизированы специфика и направленность информационных атак, которым подвергается Республика Беларусь. Показана роль в этих акциях твиттер-технологий и информационных сетей. Раскрыта структурная архитектоника информационных атак, их составных компонентов. Сконструированы теоретические модели составных компонентов информационной войны, использования информационного оружия в современном идеологическом противоборстве, а также средств и методов, применяемых в нем. Выявлены особенности и основные направления обеспечения информационной безопасности как важного фактора устойчивого развития страны. Сформулированы основные направления обеспечения информационной безопасности Беларуси.

Вступление человечества во второе десятилетие XXI века резко выявило тенденцию к обострению глобальной нестабильности, ужесточению конфликта интересов и конкуренцию моделей будущего. Убедительным подтверждением этому являются инициированные США и их союзниками по НАТО кровавые вооруженные столкновения в широких геополитических просторах «огненной дуги», включающей в себя Египет, Тунис, Ливию, Сирию, Йемен и другие страны Северной Африки. Вся эта крупномасштабная акция подготовлена и сопровождается организованными информационными атаками на правящие режимы североафриканских стран.

Исходным теоретическим и геополитическим обоснованием ведущихся такого рода информационных атак является утвержденная еще в декабре 1992 года Министерством обороны США директива под названием «Информационная война». *Информационная война – это использование собственных информационных ресурсов для идеологического воздействия на соперника (противника), ориентированное на разрушение, искажение и использование враждебной информационной системы для достижения собственных стратегических целей.*

Материально-технической базой ведения такой войны являются постоянно растущие военные расходы США, которые превышают 50% мировых затрат на эти цели, составляя около 720 миллиардов долларов в год. Эта гигантская военная машина нуждается в активных действиях, а одной из актуальных форм такой активизации являются информационные атаки, осуществляемые практически (может быть кроме Австралии) на всех континентах земного шара. Широко известны информационные атаки, предпринятые США и их соющзниками по НАТО против Ирака, Югославии, Грузии, Украины, Кыргызстана, целого ряда североамериканских стран. В эту орбиту более или менее регулярно попадает и Республика Беларусь. Достаточно вспомнить сопровождаемые разнузданной пропагандой неоднократные экономические и политические санкции против нашей страны. Эти информационные атаки были ориентированы на дискредитацию Беларуси и выдавливание ее из общеевропейской политики, на подрыв суверенитета и национальной безопасности независимого государства.

В условиях осуществления перехода Беларуси в фазу постиндустриального, информационного развития приоритетное значение приобретает обеспечение информаци-

онной безопасности страны. *Информационная безопасность* воплощается в способности государства, общества, социальной общности, личности обеспечить защищенность информационных ресурсов, необходимых для поддержания своей жизнедеятельности, устойчивого функционирования и развития, эффективно противостоять информационным опасностям и угрозам. Она включает в себя поддержание постоянной готовности к адекватным мерам в информационном противоборстве, государственную и судебную защиту государственных и частных банков данных, средств обработки, хранения и передачи информации, охрану интеллектуальных ресурсов и поддержку их всемерного развития и реализации в различных сферах жизнедеятельности общества.

Судя по всему использование информационных технологий и социальных сетей в информационном противоборстве будет неуклонно нарастать. Так, Госсекретарь США Хилари Клинтон, выступая в феврале 2011г. с речью о состоянии интернет-свобод в мире, утверждала, что в Вашингтоне именно «интернет считают важнейшим инструментом по экспорту демократии». По ее словам, социальные сети, в частности «Твиттер» и «Facebook», предоставляют людям возможности для самовыражения и администрация Барака Обамы будет широко оказывать поддержку политически активным деятелям Интернета в странах, где ущемляются права и свободы граждан, помогая им технически быть на шаг впереди цензоров». В 2011 г. на поддержку активных сетевых блоггеров в странах с так называемым авторитарными режимами Госдепартамент США намечает выделить 25 млр. долларов. Фактически эта громадная сумма направляется на подрыв информационной и политической безопасности неугодных Соединенным Штатам политических режимов.

Следует иметь в виду, что в первом десятилетии XXI века создается и стремительно расширяется новейший технологически мощно оснащенный фронт организации информационных атак на неугодные американским миллиардерам и их ставленникам политические режимы, базирующихся на так называемых *твиттер-технологиях*. Твиттер, созданный в 2006 году, – это социальная сеть, построенная на микроблогах, кратких сообщениях, ограниченных, как правило, 140 символами (одно SMS-сообщение). В таких твиттерах за внешне безобидным стремлением поболтать с другим пользователем сети в любой момент времени и в любой точке планетарного пространства скрываются широкие возможности почти мгновенной пердачи разнообразной информации, в том числе и в интересах развертывания и активного проведения информационных войн. О том, каких масштабов способно достичь использование твиттер-технологий в разворачивании информационной (и не только) войны, свидетельствуют так называемые «революции», прокатившиеся в январе–марте 2011 года по огромной огненной дуге социально-политических потрясений и вызванное ими крушение правящих режимов в ряде североафриканских стран: Египте, Тунисе, Йемене, Алжире, Бахрейне, Иордании, Ливии. Эти трагические события были заранее спланированы, подготовлены и профинансированы спецслужбами США и обученными ими специалистами по взламыванию существующих в той или иной стране социально-политических порядков.

Об этом с циничной откровенностью до свершения названных событий говорилось на сайтах знаменитого Wikileaks и в других средствах информации. Уже в ходе самих этих сетевых революций на сайте «Голоса Америки» можно было лицезреть видеоролик с откровениями бывшего египетского полицейского, завербованного спецслужбами США и проживающего недалеко от Вашингтона, о том, как он через твиттер-технологии в январе–феврале 2011 года выводил на площади Каира тысячи египтян для свержения режима Мубарака. Многие серьезные аналитики как в западных странах, так и в России прямо пишут о том, что «сетевые революции» в североарфиканских странах начали готовиться уже в первые месяцы прихода Обамы в Белый дом, что именно он является главным режиссером этих политических переговоров

(С. Кургинян: Обама снимает маску и приступает к глобальному переделу мира // Комсомольская правда. – 2011. – 24 февраля–2 марта). Главная цель «сетевых революций» – восстановить американские «правила игры», взять под контроль будущие движения капитала и будущие энергетические потоки не только исламского мира, но и Китая, России, Европейского союза. Речь идет фактически о глобальной трансформации мироустройства под эгидой США.

Не нужно быть крупным пророком, чтобы предвидеть, что активно используемые правящими кругами США твиттер-технологии и вики-микс-компромат обрушатся в недалеком будущем на Среднюю Азию, некоторые страны, которые входят в состав ОДКБ, следовательно, такие твиттер-атаки не могут оставить сторонними наблюдателями и граждан нашей страны, которая является ныне председателем в ОДКБ. Нашим специалистам в области информационной безопасности следует быть готовыми к подобного рода разворотам событий. Следует иметь в виду, что с марта текущего года госдепартамент США активизировал работу в социальных сетях для реализации проектов по вербовке русскоязычных блоггеров для «продвижения демократии в России и Беларуси». Следует обратить внимание на то обстоятельство, что, по словам основателя «Викиликс» Джулиана Ассанжа, Интернет – это величайшая шпионская машина, которую когда-либо использовал мир. О грандиозных масштабах этой деятельности свидетельствует, например, такая цифра: Агентство национальной безопасности перехватывает около 650 миллионов коммуникаций во всем мире для обслуживания своих целей посредством анализа социальных сетей.

Исходя из этого следует рассматривать и оценивать социальные сети как мощное техническое средство, создающие возможности для осуществления при их помощи серьезных угроз национальной безопасности. Особенно это становится актуальным в преддверии парламентских выборов в нашей стране 2012 г., когда наверняка активизируются попытки враждебных сил дестабилизировать информационную и политическую ситуацию в республике. В связи с этим необходимо охарактеризовать основные части информационной войны, которая периодически становится против нашей страны то более, то менее интенсивной. Структурная архитектоника информационных атак сводится к шести взаимосвязанным компонентам (рисунок 1):

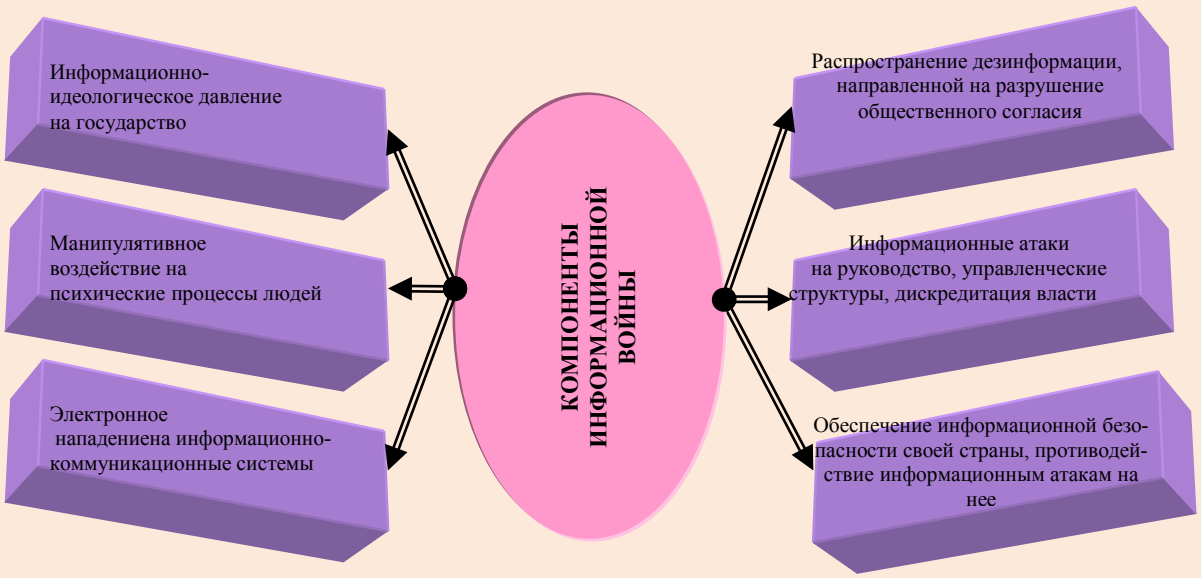

Рисунок 1 – Составные компоненты информационной войны

1. Обеспечение информационно-идеологического давления на враждебное государство в целях подрыва психологической и духовной обстановки в стране, разрушения в ней традиционных культурных, нравственных, эстетических ценностей.

2. Организация психологических операций, направленных на осуществление манипулятивного целенаправленного воздействия на сознательные и бессознательные психические процессы населения определенной страны, на его эмоции, чувства, волевые импульсы, ценностные ориентации и жизненные стратегии с целью изменить их в желаемом для инициаторов информационных атак направлении.

3. Осуществление электронного нападения на информационно-коммуникационные системы страны-соперника, на его компьютерные системы и сети с целью ослабить, дезорганизовать или разрушить эту систему, не позврлить сопернику получать оперативную и достоверную информацию о состоянии и использовании своих собственных экономических, военных и иных ресурсов, а также ресурсах и действиях враждебной стороны.

4. Распространение дезинформации, т.е. недостоверной и/или умышленно-искаженной информации, направленной на разрушение общественного согласия, на дискредитацию действующих в стране системы власти и политических институтов, разжигание социальной розни, национальной и религиозной вражды, предоставление сопернику ложной информации о собственных целях, намерениях и силах.

5. Прямые информационные атаки на руководство, управленческие структуры страны-соперника, ее экономическую, политическую системы, ее культурное достояние и систему безопасности во всех ее видах – политическую, военную, продовольственную, экологическую, информационную и т.п.

6. Обеспечение мер безопасности в информационной сфере, включая эффективное использование информационных ресурсов страны, их сохранность и расширенное воспроизводство, защиту сведений, составляющих государственную, служебную, коммерческую и иную охраняемую законодательством тайну, разоблачение прямых информационных атак на свою страну, активное и эффективное противодействие им.

Применительно к сфере идеологического влияния на людей можно сказать, что информационная война – это деятельность, направленная на завоевание общественного мнения, внедрение в него определенных идей, ценностных ориентаций, оценок, стандартов поведения, преследующая цель – установление контроля над массовым сознанием, над эмоциями масс в своих собственных интересах.

Каковы составные компоненты информационной войны?

В таких информационных войнах нередко применяются не только различные способы манипулирования сознанием людей, их деформации, но и такие грязные технологии, как промышленный шпионаж, кражи и несанкционированное копирование информации с электронных носителей для различного рода идеологических компроматов. Все это используется для последующего подкупа, вербовки, угроз или шантажа. Вследствие этого одной из основных составляющих информационной войны становится специфическое противостояние алгоритмов и технологии, идей, материализованных в информационных устройствах и средствах, предназначенных для нанесения экономического, политического, финансового, психологического и иного ущерба противнику или конкуренту, и, прежде всего, их информационным и телекоммуникационным системам. Наиболее опасным из перечисленных направлений такой войны является возможность применения способов воздействия на психику человека помимо его воли. Возможность отрицательного воздействия информации на мозг человека создает предпосылки для производства психологического (психотропного) оружия, которое атакует подкорку головного мозга специальными информационными полями. Такие атаки целенаправленно используются

для скрытого изменения человеческого сознания, поведения и здоровья с целью решения задач политического, военного, экономического, информационного характера.

В соответствии с замыслами и целями идеологического противоборства формируется комплекс взаимосвязанных задач, которые должны быть решены с помощью информационного оружия. Вот некоторые, наиболее существенные из них (рисунок 2):

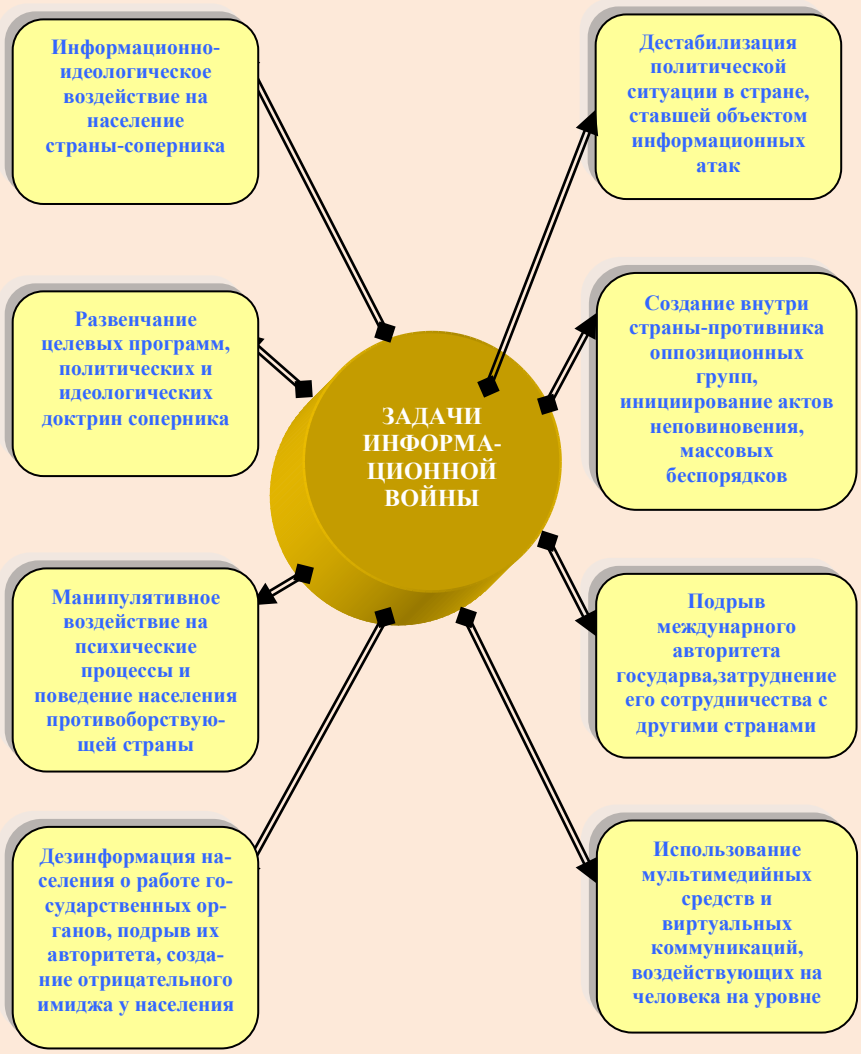

Рисунок 2 – Задачи информационной войны

1. Активное явное и латентное (скрытое информационно-идеологическое воздействие на население страны-соперника, на его сознание, чувства, ценностные ориентации и смысложизненные установки, ориентированное на создание в ней атмосферы бездуховности, безнравственности, беспринципности.

2. Развенчание целевых программ, политических лозунгов, идеологических доктрин, используемых соперничающей стороной с целью создания в этой стране политической напряженности и хаоса.

3. Применение манипулятивных способов воздействия на психические процессы и поведенческие акты, характерные для населения противоборствующей страны.

4. Дезинформация населения о работе государственных органов, подрыв их авторитета, дискриминация деятельности всех уровней и звеньев управленческих струк-

тур создание их отрицательного имиджа у населения с целью затруднения принятия органами управления важных решений.

5. Дестабилизация политической ситуации в стране, ставшей объектом информационных атак с целью провокации конфликтов, разжигания недоверия, подозрительности, обострения политической борьбы.

6. Поддержка внутри страны противника оппозиционных групп, инициирование забастовок, актов неповиновении, массовых беспорядков и других акций социально-экономического и политического протеста.

7. Подрыв международного авторитета государства, затруднение его сотрудничества с другими странами.

8. Использование мультимедийных средств в виде информационно-развлекательных или аналитических страниц с «сенсационной» или иной «горячей» информацией, составленных с учетом особенностей восприятия человека и психологии виртуальных коммуникаций, что позволяет оказывать глубинное, чаще всего на уровне подсознания, воздействие на человека, воспринимающего такую информацию.

Для решения этого широкого круга задач применяются, как правило, довольно разнообразные средства и методы. Наиболее часто используемые из них можно изобразить таким образом, как это показано на рисунке 3:

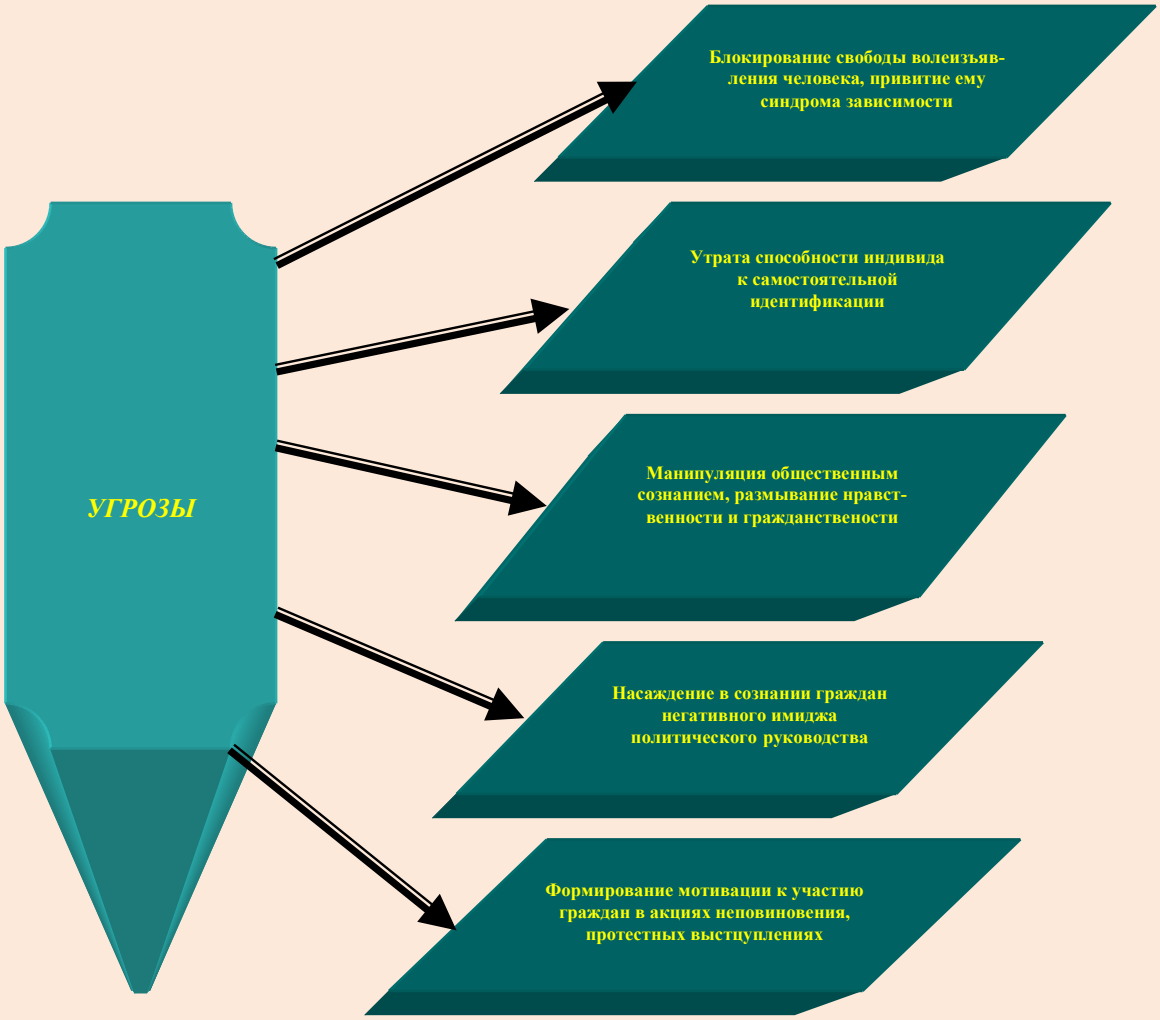

Рисунок 3 – Средства и методы, применяемые в информационной войне

Весь охарактеризованный ряд средств, применяемых в процессе информационного противоборства, находит в разных сочетаниях и в разных пропорциях воплощение в тех идеологических атаках, которые организуют против Беларуси, ее народа и государства наши заокеанские и западноевропейские недруги и их доморощенные приспешники. Поэтому ни в коем случае нельзя недооценивать те угрозы, которые возникают в этой важной сфере национальной обороны. Несмотря на огромные суммы финансирования из-за рубежа старания и поборников оппозиционных экстремистов уровень протестного потенциала и протестной активности граждан Беларуси остается низким. Если взять последние два года, то динамика роста протестных акций и их участников не наблюдается. Число таких участников очень редко достигает 120 человек. Даже провалившаяся попытка насильственной «цветной революции» 19 декабря 2010 г. собрала всего около трех тысяч человек. Готовность наших сограждан участвовать в протестных мероприятиях следует считать низкой, поскольку 88% населения республики отрицают такую возможность даже в исключительных случаях.

Последняя акция протестных активистов, которые обещали 8 октября этого года вывести на площадь для участия в широко разрекламированной в иностранной и оппозиционной прессе в многочисленных листовках, эсэмэсках, для рассылки которых затрачено свыше 30 тыс. евро, в десятках городов огромное количество людей, в том числе в Минске – 100 тыс. человек, окончилась сокрушительным провалом. На площади Бангалор для участия в широкоосвещаемом « народным сходе» собралось всего около 120 человек. А инициаторы этого сборища В. Некляев, Римашевский, Калякин сокрушались в интервью иностранным корреспондентам по поводу дождливой и холодной погоды и неготовности белорусского народа жить в условиях демократии.

Характеризуя информационную обстановку в Беларуси в целом, следует отметить, что государственные СМИ сохраняют доминирование в национальном медиапространстве. Средний показатель уровня доверия населения к государственным телеканалам составляет 56,7%. Основные печатные государственные СМИ удерживают влияние около 86% телевизионной аудитории. Уровень доверия информации, распространяемый республиканскими и местными радиоканалами, составляет 53–59% радиоаудитории. На этом фоне гораздо слабее выглядят позиции государственных органов в сети Интернет, где нередко преобладают так называемые «независимые» информационно-новостные ресурсы. К тому же и качество работы государственных органов в Интернете на фоне стремительных темпов роста сетевой аудитории остается недостаточным. Они зачастую оказываются плохо подготовленными к ведению эффективного противоборства, в том числе с использованием информационных современных технологий.

В этой сфере следует иметь в виду возможности расширения информационных атак на нашу страну, что связано с тремя обстоятельствами:

1) усиление западного информационного прессинга в связи с подготовкой к выборам в белорусский парламент в 2012 г.;

2) значительное большинство белорусских масс-медиа отстает от зарубежных по качеству подготовки и подачи материалов;

3) наращивание масштабов, качества, каналов оппозиционной пропаганды.

Следует иметь в виду, что основное усилие информационных атак, ведущихся против нашей страны, направлено на микросоциальные аспекты безопасности. Центром их внимания становится жизнь человека, его смысложизненные интересы и ценности. Поэтому исходным пунктом системного понимания и обеспечения безопасности в информационной сфере является безопасность личности. Обеспечение личной безопасности осуществляется посредством решения ряда конкретных задач, имеющих систематический превентивный аспект и связанных с выявлением и предотвращением

угроз и опасностей, возникающих в разнообразных кризисных и конфликтных ситуациях, затрагивающих жизненно важные интересы человека. Обеспечение безопасности личности – это, в конечном счете, создание и функционирование благоприятной для человека внутренней и внешней среды, это гармоничное развитие самого человека, это его благоприятное самочувствие, это реализованная способность человека во всех условиях оставаться самим собой, сохранять свою самобытность и личное достоинство, это высокое качество жизни, которое определяется не только материальным и культурным благосостоянием человека и его семьи, но и ощущением полноты жизни и осознанием ее смысла.

Во втором десятилетии XXI века информационная сфера превращается в системообразующий фактор жизнедеятельности людей, устойчивого развития общества и государства. Широкое применение информационных технологий открывает беспрецедентные возможности научно-технологической, образовательной, управленческой деятельности, но одновременно создает и технологическую базу для обострения информационного противоборства и злонамеренных воздействий на личную и государственную безопасность в ущерб национальным интересам суверенных стран. В таких условиях проведение разнообразных мероприятий по усилению информационной безопасности следует концентрировать на следующих основных направлениях (рисунок 4):

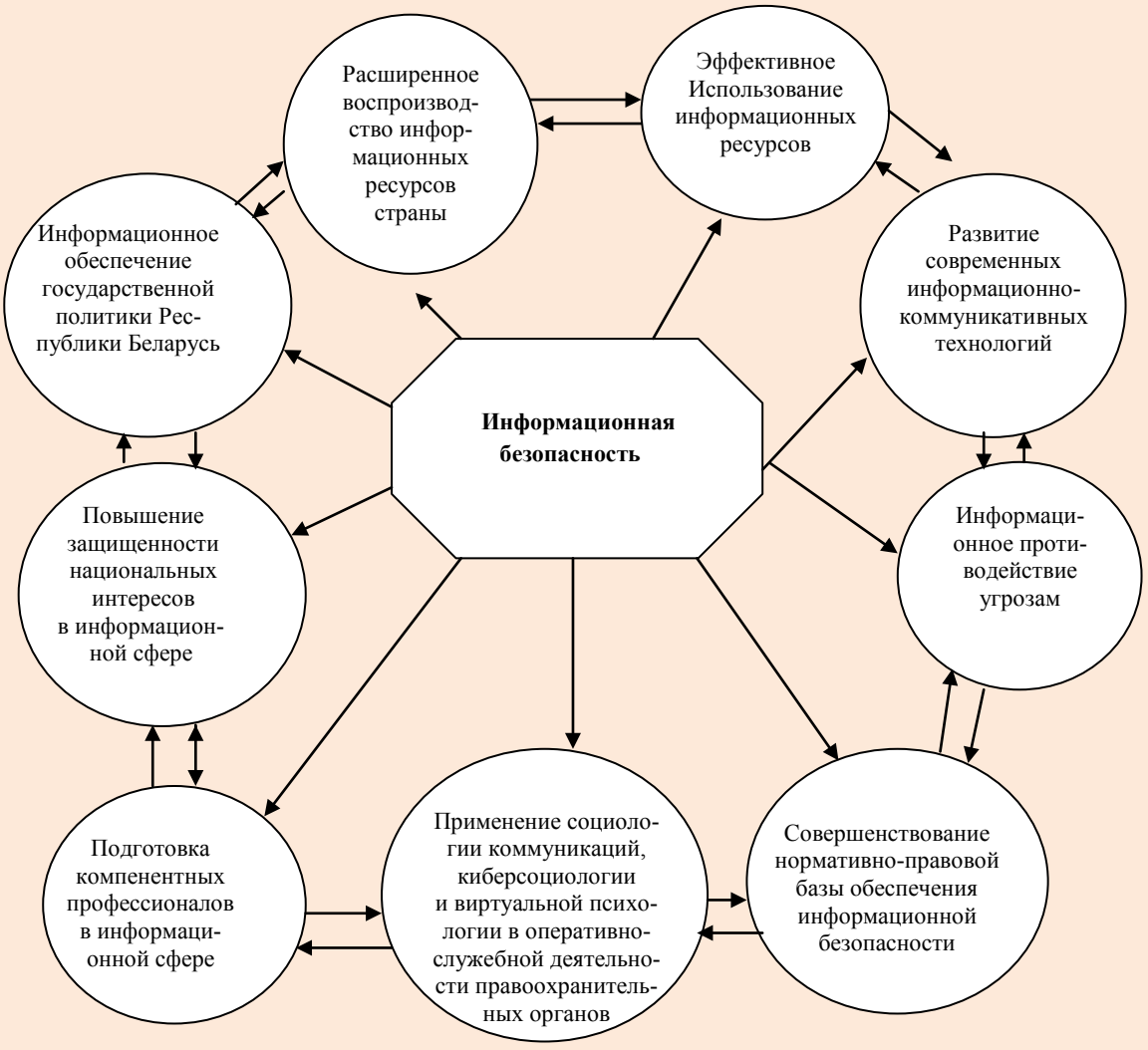

Рисунок 4 – Основные направления обеспечения информационной безопасности Беларуси

1) Сохранность, приумножение и расширенное воспроизводство информационных ресурсов страны.

2) Эффективное использование информационных ресурсов.

3) Информационное обеспечение государственной политики Республики Беларусь, связанное с доведением до белорусской и международной общественности достоверной информации о стратегической цели и основных приоритетах деятельности белорусского государства с обеспечением доступа граждан к открытым государственным информационным ресурсам.

4) Развитие современных информационно-коммуникативных технологий, отечественной индустрии информации и их эффективное использование для упрочения информационной безопасности страны.

5) Повышение защищенности национальных интересов в информационной сфере.

6) Информационное противодействие внешним и внутренним угрозам конституционным правам и свободам человека в области духовной жизни, гражданской деятельности и информационных коммуникаций.

7) Подготовка компетентных специалистов в области развития, совершенствования и защиты информационно-коммуникационных систем.

8) Применение достижений социологии коммуникаций, кибер-социологии и виртуальной психологии в оперативно-служебной деятельности правоохранительных органов страны.

9) Совершенствование нормативной правовой базы обеспечения информационной безопасности, в том числе путем оптимизации социальных механизмов регулирования всех видов деятельности в этой сфере.

Таковы основные аспекты обеспечения информационной безопасности белорусского общества в условиях противоречиво развивающейся глобализации и становления нелинейно развивающегося мира.

Babosov E.M. **Provision of Information Security as a Factor for SustainableDevelopment of Belarus**

It is noted in the article that in conditions of global instability aggravation and conflict of interests of different countries and coalitions in the second decade of the XXI century perspective of information security providing across the Eurasian continent becomes actual. The essence and characteristics of information warfare, its basic form in today's uncertain world are characterized from this point of view. In this context specificity and direction of information attacks that Belarus run the danger of are classified. The role of tweeter technology and information networks in the process is showed. Structural architectonics of information attacks and their constituent components are revealed. Theoretical models of composite components of information warfare, the use of information warfare in the modern ideological confrontation and the means and methods that are used in it are constructed. The features and main directions of information security as an important factor for sustainable development are characterized. The basic directions of information security in Belarus are defined.

Рукапіс паступіў у рэдкалегію 02.03.2012