

Кучерявый М. М., Вовенда Ю. В.

Региональная информационная безопасность в рамках евразийской интеграции

Кучерявый Михаил Михайлович

Руководитель Управления Федеральной службы по техническому и экспортному контролю России по Северо-Западному Федеральному округу (Санкт-Петербург)
Доктор политических наук
szfo@fstec.ru

Вовенда Юлия Владимировна

Управление Федеральной службы по техническому и экспортному контролю России по Северо-Западному федеральному округу (Санкт-Петербург)
Ведущий специалист-эксперт
Аспирант кафедры международных отношений СЗИУ РАНХиГС
vovenda-yv@sziu.ru

РЕФЕРАТ

В статье рассматриваются проблемы обеспечения информационной безопасности стран евразийского пространства. Освещаются основные положения проекта новой редакции Доктрины информационной безопасности Российской Федерации и Стратегии национальной безопасности РФ, касающиеся обеспечения информационной безопасности. Особое внимание уделено системе защиты информации Северо-Западного федерального округа Российской Федерации и Единой региональной политике информационной безопасности на евразийском пространстве.

КЛЮЧЕВЫЕ СЛОВА

информационная безопасность, национальная безопасность, информационно-коммуникационные технологии, угрозы национальной безопасности, Евразийский регион

Kucheryavyy M. M., Vovenda Yu. V.

Regional Information Security within the Framework of the Eurasian Integration

Kucheryavyy Mikhail Mikhailovich

The Chief of headquarters in the North-West Federal District of the Federal Service for Technical and Export Control (Saint-Petersburg, Russian Federation)
Doctor of Political Science
szfo@fstec.ru

Vovenda Yulia Vladimirovna

Headquarters in the North-West Federal District of the Federal Service for Technical and Export Control (Saint-Petersburg, Russian Federation)
Leading specialist expert
Graduate student of Chair of the International Relations of North-West Institute of Management — branch of the Russian Presidential Academy of National Economy and Public Administration (Saint-Petersburg, Russian Federation)
vovenda-yv@sziu.ru

ABSTRACT

The article is considered the problems of information security Eurasian countries. Highlights the main provisions in the framework of information security the new draft of the Doctrine of Information Security of the Russian Federation and the US National Military Strategy. The main attention is paid to information security of North-West Federal District of the Russian Federation and the United Regional Policy Information Security in Eurasia.

KEYWORDS

information security, national security, information and communication technologies, threats of national security, Eurasian region

В современном мировом сообществе в настоящее время сформировались и крайне обострились противоречия между ведущими мировыми державами в политической, экономической, идеологической, информационной и военной областях. Данные противоречия привели к увеличению числа угроз в перечисленных областях и, как следствие, разрешение противоречий происходит в ходе ведения вооруженной борьбы в наземной, морской, воздушно-космической и информационной сферах.

Эскалация существующих вооруженных конфликтов в регионах Ближнего и Среднего Востока и севере Африканского континента, рост числа подготовленных и спровоцированных фактов международного терроризма с гибелью людей в конечном итоге могут привести к их перерастанию в локальные, а возможно, и региональные войны.

США и страны Запада оказывают постоянное давление на Российскую Федерацию с целью заставить нашу страну отказаться от политики проведения своих национальных интересов по оказанию существенного влияния на военно-политические и экономические события современного глобального мира, прежде всего, в странах бывшего СССР, Ближнего Востока, Азиатском и Африканском континентах [5, с. 6].

В связи с этим на первый план выдвигаются вопросы реализации государственной политики в области защиты суверенитета, территориальной целостности и конституционного строя Российской Федерации с учетом существующих и возможных угроз национальной безопасности. В данных условиях Советом Безопасности России в 2015 г. была подготовлена и проработана новая редакция Стратегии национальной безопасности Российской Федерации до 2020 г. и продолжается активная работа по согласованию новой редакции Доктрины информационной безопасности страны.

В новой редакции Доктрины отмечается, что «информационные и коммуникационные технологии не только позитивно влияют на развитие экономики и совершенствование функционирования общественных и государственных институтов, но и порождают новые вызовы и угрозы национальной безопасности. Это обусловлено тенденцией к использованию информационного пространства для решения военно-политических задач, а также террористических и иных противоправных целей»¹. Неоспорим факт наращивания зарубежными странами возможностей по использованию достижений информационно-коммуникационных технологий (ИКТ) для воздействия на критическую информационную инфраструктуру России с целью вывода из строя или затруднения ее работоспособности. Необходимо отметить, что спецслужбы, подконтрольные общественные организации США и стран НАТО используют ИКТ «в качестве инструмента для подрыва суверенитета и нарушения территориальной целостности других государств, дестабилизации внутриполитической и социальной ситуации», а также для «наращивания информационного воздействия на население страны, в первую очередь на молодежь, с целью размывания культурных и духовных ценностей, подрыва нравственных устоев, исторических основ и патриотических традиций»².

В Стратегии национальной безопасности РФ, которая введена в действие с 31 декабря 2015 г., сказано, что «проведение Российской Федерацией самостоятельной внешней и внутренней политики вызывает противодействие со стороны США и их союзников, стремящихся сохранить свое доминирование в мировых делах. Реали-

¹ Доктрина информационной безопасности Российской Федерации. Новая редакция // [Электронный ресурс]. URL: http://infosystems.ru/assets/files/files/doktrina_IB.pdf (дата обращения: 20.06.2016).

² Там же.

зубаемая ими политика сдерживания России предусматривает оказание на нее политического, экономического, военного и информационного давления»¹.

Для того чтобы противостоять внешним и внутренним угрозам, в Российской Федерации создана и действует система обеспечения национальной безопасности России (рис. 1). Система обеспечения национальной безопасности включает: высшее политическое руководство страны; федеральные министерства, службы и агентства с их территориальными органами в регионах; различные по форме создания и содержанию работы общественные организации и объединения с представительскими в регионах; а также граждан России, участвующих в защите национальных интересов, и одновременно являющимися организаторами процессов стабилизации в областях общественных отношений.

В сегодняшнем глобальном мире устремления международного терроризма, как одной из основных угроз безопасности России, направлены на установление господства на значительных территориях Евразийского и Африканского континентов. Прошедший 2015 г. и начало 2016 г. отмечены ростом масштабных террористических актов с большим числом человеческих жертв: подрыв в воздухе российского пассажирского самолета А321 30 октября привел к гибели 224 пассажиров и членов экипажа; взрывы 13 ноября в Париже — 132 погибших и более 300 раненых; 30 человек погибли при захвате отеля в Буркина-Фасо 16 января текущего года; есть и другие факты гибели людей от рук террористов.

Ударом в спину назвал Президент Российской Федерации В. В. Путин неправомерные действия ВВС Турции 24 ноября по сбитию российского фронтового бомбардировщика СУ-24М, выполнявшего боевую задачу в Сирийской Арабской Республике по уничтожению объектов международной террористической организации ИГИЛ. В настоящий момент террористическая организация Исламское государство Ирака и Леванта (ИГИЛ или в арабских средствах массовой информации — ДАИШ), запрещенная на территории Российской Федерации, осуществила захват и контролирует некоторые районы Сирии и Ирака, а также ведет боевые действия в Алжире, Ливии, Египте, Йемене, Турции, Афганистане, Пакистане, Мали.

Ситуация в области противодействия терроризму в Российской Федерации остается достаточно сложной в связи с продолжающейся деятельностью бандформирований на Северном Кавказе, распространением идеологии терроризма в социальных сетях, активизацией деятельности международных террористических организаций особенно после результативных боевых действий Воздушно-космических сил России [3, с. 165].

В данных условиях с целью обеспечения международной безопасности Россия проводит целенаправленную политику на дальнейшие интеграционные процессы в области экономики, политики, военной и информационной безопасности в Евразийском регионе.

Формирование Евразийского экономического союза (ЕАЭС) проходит в условиях явной геополитической нестабильности. «Поддержка США и Европейским союзом антиконституционного государственного переворота на Украине привела к глубокому расколу в украинском обществе и возникновению вооруженного конфликта на ее Юго-Востоке. Укрепление крайне правой националистической идеологии, целенаправленное формирование у украинского населения образа врага в лице России, неприкрытая ставка на силовое решение внутригосударственных противоречий, глубокий социально-экономический кризис превращают

¹ Указ Президента Российской Федерации от 31 декабря 2015 г. № 683 «О стратегии национальной безопасности Российской Федерации» // [Электронный ресурс]. URL: <http://m.rg.ru/2015/12/31/nacbezopasnost-site-dok.html> (дата обращения: 20.06.2016).

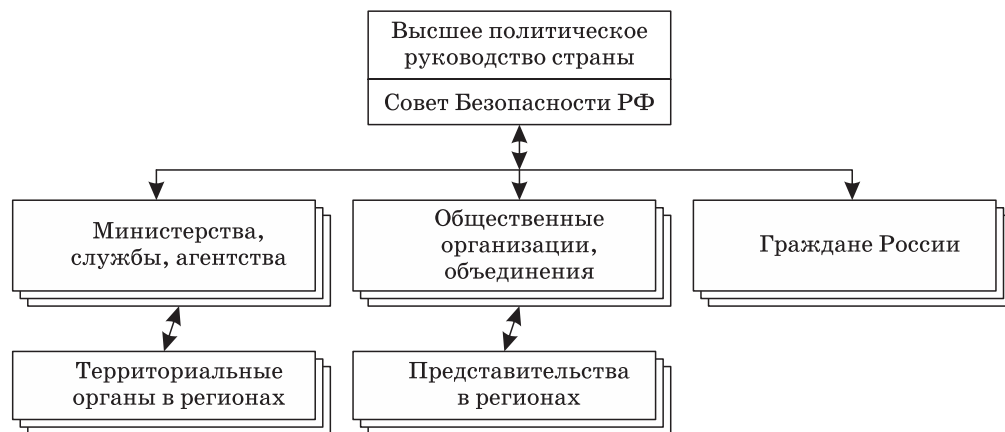


Рис. 1. Система обеспечения национальной безопасности

Украину в долгосрочный очаг нестабильности в Европе и непосредственно у границ России»¹.

Результатом обострения данного конфликта стало введение санкций со стороны США и Западных стран в отношении России. В настоящий момент все усилия стран-участниц ЕАЭС направлены на развитие экономического сотрудничества, однако в перспективе данный союз станет основой для создания новой политической организации. Можно полагать, что в перспективе совместно с Россией, Казахстан, Белоруссия, Киргизия, Армения, а также возможные новые члены союза, смогут проводить не только согласованную экономическую, но и внешнеполитическую линию [2, с. 107]. Формирование ЕАЭС, наряду с действующими ШОС и БРИКС, может создать объективные предпосылки для образования нового полюса силы в мировом сообществе, что в свою очередь приведет к становлению в ближайшие 7–10 лет многополярного мира.

Российская Федерация является локомотивом продвижения евразийской интеграции на новый уровень и инициатором окончательного оформления ЕАЭС в качестве экономического и политического союза. В ближайшей перспективе возможна организация взаимовыгодного сотрудничества ЕАЭС с Европейским союзом в экономической сфере [1, с. 103]. Предпосылки для этого есть: политическая и бизнес элита Европейского союза уже на данном этапе отчетливо осознают экономические преимущества сотрудничества с ЕАЭС, а также наличие заявлений глав ряда европейских государств о намерениях полностью снять экономические санкции с Российской Федерации в ближайшие годы.

В зарубежных средствах массовой информации наблюдается тенденция увеличения объема материалов, которые содержат необъективную или предвзятую информацию о внешней и внутренней политике России, о деятельности государственных структур, в частности, руководства страны и вооруженных сил.

Одновременно с этим наблюдается рост количества компьютерных атак на информационно-телекоммуникационные сети и информационные системы органов власти. В настоящее время не решена проблема защиты государственных информационных систем, где по-прежнему используется программное обеспечение иностранных компаний. Поэтому организационные и технические системы защиты

¹ Указ Президента Российской Федерации от 31 декабря 2015 г. № 683 «О стратегии национальной безопасности Российской Федерации».

информации в настоящее время требуют постоянного совершенствования и обновления, а также перехода на отечественную продукцию, в рамках программы импортозамещения.

В Северо-Западном федеральном округе Российской Федерации организована и проводится активная работа по обеспечению защиты информации в государственных информационных системах¹. Центральные органы власти уделяют должное внимание данной проблеме, о чем свидетельствует проведение в июле 2015 г. в Вологде выездного совещания Совета Безопасности Российской Федерации, где принято решение об активизации деятельности должностных лиц, органов государственного и военного управления по прогнозированию, выявлению и оценке угроз информационной безопасности Российской Федерации на Северо-Западе, на анализ состояния и перспектив развития военно-политической и социально-экономической ситуации в регионе, а также на необходимость принятия неотложных мер по совершенствованию системы подготовки кадров в области информационной безопасности.

С учетом особенностей Северо-Западного округа (непосредственно граничит со странами-членами блока НАТО; наличие значительного количества предприятий оборонно-промышленного комплекса, производящих современные образцы вооружений и военной техники; наличие стратегических и оперативных объединений и соединений, а также систем управления Вооруженными Силами России) с целью противодействия средствам иностранных технических разведок и обеспечения информационной безопасности округа создана система защиты информации, которая интегрирована в общую систему безопасности государства (рис. 2).

Система защиты информации является многоуровневой и включает в себя: межрегиональный, региональный и объектовый уровни.

Общее руководство системой защиты информации в округе осуществляют полномочный представитель Президента Российской Федерации через Межведомственный совет по защите информации. В субъектах Российской Федерации — главы субъектов и комиссии по защите информации. В органах власти и организациях ответственность за обеспечение защиты информации возлагается на их руководителей.

Регулятором в области защиты информации и организатором функционирования данной системы в рамках округа является Управление Федеральной службы по техническому и экспортному контролю по Северо-Западному федеральному округу.

Система защиты информации округа развивается и совершенствуется с учетом расширения возможностей угроз, исходящих со стороны технических разведок иностранных государств, и возрастания масштабов информатизации органов власти и организаций.

Эффективное управление этой системой обеспечивается координацией работ по защите информации в оборонной, политической сферах по следующим направлениям:

- 1) проведению оценки угроз информационной безопасности объектам защиты округа;
- 2) планированию и реализации организационно-технических мероприятий по предотвращению угроз;
- 3) координации деятельности федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и органов местного самоуправления в области обеспечения информационной безопасности;
- 4) обеспечению информационной безопасности критически важных объектов;
- 5) кадровому и нормативно-правовому обеспечению информационной безопасности.

¹ Об информации, информатизации и защите информации: Федеральный закон от 20 февраля 1995 г. № 24-ФЗ // [Электронный ресурс]. URL: <http://base.garant.ru/70687520> (дата обращения: 20.06.2016).

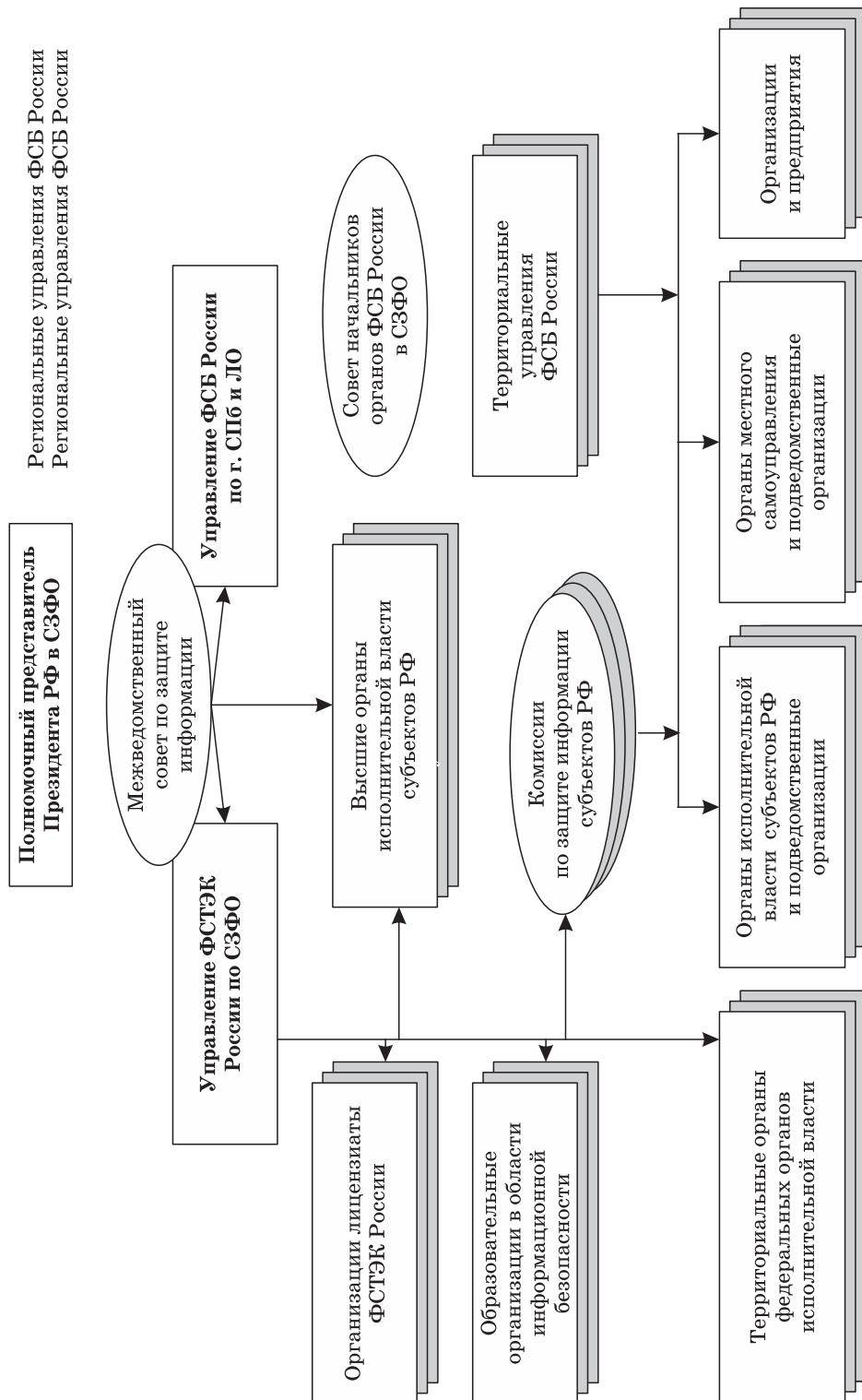


Рис. 2. Система защиты информации в Северо-Западном федеральном округе

Глобализация современного мира приводит к усилению угроз в информационной сфере, уязвимости информационных систем органов государственной власти и военного управления не только отдельных государств, но и межгосударственных образований.

В условиях евразийской интеграции необходимо проводить единую региональную политику информационной безопасности [4, с. 126]. Для эффективного проведения такой политики необходимо выработать комплексный подход, который будет основываться на развитии следующих направлений: информационно-политическое, информационно-технологическое и информационно-психологическое.

Совместная информационная деятельность государств — членов ЕАЭС и ОДКБ в сфере обеспечения информационной безопасности имеет своей целью более эффективную защиту их законных интересов в информационном пространстве. Формирование единого органа коллективной безопасности, скоординированной информационной политики государств — членов ЕАЭС и ОДКБ — важные приоритетные направления противодействия современным вызовам и угрозам. Взаимодействие в рамках ЕАЭС подразумевает унификацию законодательств в экономической сфере, для более четкого ответа на информационные вызовы и угрозы со стороны внешней среды необходимо разработать единую политику безопасности на основе Доктрины информационной безопасности Российской Федерации, сформировать объединенную систему информационного противоборства.

В проекте новой редакции Доктрины информационной безопасности отмечается, что «в экономической области сохраняется отставание Российской Федерации от ведущих зарубежных государств в создании конкурентоспособных информационных технологий и продукции на их основе, что обуславливает зависимость Российской Федерации от экспортной политики зарубежных стран»¹. Поэтому для эффективного проведения единой региональной политики информационной безопасности, информационно-технологическое направление должно подразумевать разработку и создание собственных информационно-коммуникационных технологий и проведение политики импортозамещения в информационной сфере. Данное направление подразумевает разработку отечественного сертифицированного программного обеспечения, региональной системы технической защиты информации.

Информационное психологическое направление включает формирование общего языка межнационального общения, разработку унифицированного понятийного аппарата и формирование единой информационной культуры, которые позволят объединить усилия, снизить затраты на противодействие угрозам, повысить эффективность мер по обеспечению информационной безопасности.

Во всех составляющих национальной безопасности — политической, экономической, военной, правоохранительной, экологической и других — вес информационных факторов непрерывно растет. Информационно-психологическое воздействие, которое реализуется через средства массовой информации, могут создать атмосферу напряженности и политической нестабильности в обществе, спровоцировать социальные, национальные, религиозные конфликты и массовые беспорядки, привести к разрушительным последствиям для демократического развития страны. Незаконное использование, хищение или искажение деловой (банковской, коммерческой, статистической) информации неизбежно ведут к тяжелым экономическим потерям. Уровень развития информационных технологий, на которых основываются современные системы разведки, радиоэлектронной борьбы существенно предопределяет исход вооруженных конфликтов. Именно поэтому национальная безопасность любой страны существенным образом зависит от обеспечения информационной безопасности, причем в ходе технического прогресса эта зависимость будет

¹Доктрина информационной безопасности Российской Федерации. Новая редакция.

еще более возрастать. Современные угрозы и вызовы, исходящие из информационного мирового пространства создают дополнительные проблемы в области обеспечения национальной безопасности. С целью противодействия данным угрозам и создана система защиты информации государства, которая должна быть построена в соответствии со стремительно меняющимися условиями современного мира.

Таким образом, в условиях евразийской интеграции обеспечение информационной безопасности приобретает особую актуальность и требует выработки новых подходов к определению общей системы политических и организационных мер для создания единого безопасного информационного пространства.

Литература

- 1 Косов Ю. В., Фролов В. Е. Интеграционные процессы евразийского региона: анализ основных этапов // Управленческое консультирование. 2013. № 10 (58). С. 101–110.
- 2 Косов Ю. В., Торопыгин А. В. Проблемы безопасности государств — членов Евразийского экономического сообщества // Управленческое консультирование. 2005. № 2. С. 100–107.
- 3 Кучерявый М. М. Основные факторы влияния политики информационной безопасности на национальную безопасность современной России // Евразийская интеграция: экономика, право, политика. 2013. № 14. С. 164–168.
- 4 Кучерявый М. М. Роль России и евразийского региона в формировании глобального подхода к обеспечению международной информационной безопасности // Евразийская интеграция: экономика, право, политика. 2012. № 12. С. 121–127.
- 5 Маринин А. Национальная военная стратегия США — 2015 // Зарубежное военное обозрение. 2015. № 12 (825). С. 3–10.

References

1. Kosov Yu.V., Frolov V.E. *Integration processes of the Eurasian region: analysis of the main stages* [Integratsionnyye protsessy evraziiskogo regiona: analiz osnovnykh etapov] // Administrative Consulting [Upravlencheskoe konsul'tirovanie]. 2013. N 10 (58). P. 101–110. (rus)
2. Kosov Yu.V., Toropygin A.V. *Problems of safety of states — members of the Eurasian economic community* [Problemy bezopasnosti gosudarstv — chlenov Evraziiskogo ekonomicheskogo soobshchestva] // Administrative Consulting [Upravlencheskoe konsul'tirovanie]. 2005. N 2. P. 100–107. (rus)
3. Kucheryavy M.M. *Major factors of influence of information security policy on a homeland security of modern Russia* [Osnovnye faktory vliyaniya politiki informatsionnoi bezopasnosti na natsional'nuyu bezopasnost' sovremennoi Rossii] // Eurasian integration: economy, law, policy [Evraziiskaya integratsiya: ekonomika, pravo, politika]. 2013. N 14. P. 164–168. (rus)
4. Kucheryavy M.M. *Role of Russia and the Eurasian region in forming of global approach to ensuring the international information security* [Rol' Rossii i evraziiskogo regiona v formirovanii global'nogo podkhoda k obespecheniyu mezhdunarodnoi informatsionnoi bezopasnosti] // Eurasian integration: economy, law, policy [Evraziiskaya integratsiya: ekonomika, pravo, politika]. 2012. N 12. P. 121–127. (rus)
5. Marinin A. *National military strategy of the USA — 2015* [Natsional'naya voennaya strategiya SShA — 2015] // Foreign military review [Zarubezhnoe voennoe obozrenie]. 2015. N 12 (825). P. 3–10. (rus)