ПОЛИТОЛОГИЯ И СОЦИОЛОГИЯ

УДК 327(470+571)

С. А. Бабуркин

Шпионаж против США в оценках американской контрразведки

В статье рассматриваются подходы американской контрразведки к анализу и оценке деятельности иностранных разведывательных служб и шпионажа против США. Особое внимание уделяется характеристике масштабов и динамики контрразведывательных угроз Соединенным Штатам, их источникам, структуре и характеру, тенденциям и перспективам дальнейших изменений.

Ключевые слова: национальная безопасность, разведка, шпионаж, контрразведка США.

S. A. Baburkin

Espionage Against the USA in Estimations of the American Counterespionage

The article is devoted to the approaches of the US counterintelligence towards analysis and assessment of foreign intelligence activities and espionage against the USA. It is focused on characteristics of dimensions and dynamics of counterintelligence threats to the United States, their sources, structures and nature, trends and forecasts of their evolution.

Keywords: national security, intelligence, espionage, US counterintelligence.

При всей значимости и остроте угрозы международного терроризма для национальной безопасности США после 11 сентября 2001 г., для американской контрразведки приоритетом остается угроза иностранного шпионажа. Руководители американской контрразведки подходят к проблеме шпионажа философски. «Шпионаж – извечная проблема. Он не был изобретением холодной войны. Он старше, чем поиск Иисусом Навином Земли Обетованной, и будет с нами вечно», – утверждал руководитель национальной контрразведки США Джоел Ф. Бреннер [2, p. 2–3]. Это, однако, не мешает им видеть, что масштабы и характер контрразведывательных угроз не остаются неизменными. От них, в свою очередь, зависят усилия, предпринимаемые в области контрразведки.

В материале, подготовленном Центром изучения разведки, отмечается, что «со времени коллапса Советского Союза в 1991 г. угроза со стороны враждебных разведывательных служб изменилась, но не исчезла. Традиционно враждебные режимы, такие как Россия и Китай, увеличили масштабы и интенсивность своих разведывательных операций против Соединенных Штатов, как и другие, более дружественные государства». Отсюда делается вывод об острой необходимости «своевременной и точной разведки, агрессивной контрразведки и эффективной безопасности» [10]. Косвенно и, конечно, лишь частично о масштабах, структуре и динамике угрозы шпионажа свидетельствует судебная практика США. С 1945 по 2008 г. за шпионаж или преступления, связанные с ним, в США было арестовано 247 человек, в среднем по четыре человека в год. При этом на 2005 и 2006 гг. пришлось по десять арестов. «Это ясный индикатор того, что шпионаж остается вполне реальной угрозой национальной безопасности США», – заключал Дэвид Мэйджор, президент Центра изучения контрразведки и безопасности, выступая на слушаниях в конгрессе США в январе 2008 г. [6, p. 2–3].

Многие из арестованных агентов иностранных разведок действовали, оставаясь нераскрытыми на протяжении долгого времени, и нанесли США «колоссальный ущерб». В качестве наиболее ярких примеров обычно упоминаются «группа Уолкера» и «группа Конрада». Первая действовала в ВМС более 17 лет и передала советской разведке криптологические материалы, которые

позволили прочитать миллион сообщений, направленных находившимся на боевом дежурстве кораблям и подводным лодкам США. Вторая «группа» за 18 лет выдала планы обороны Западной Европы. Судья, рассматривавший дело Конрада, отмечал, что, «если бы между НАТО и Варшавским пактом разразилась война, Запад ожидало бы неминуемое поражение» [2, p. 4]. Не меньший резонанс вызвал арест Олдрича Эймса – высокопоставленного сотрудника контрразведки ЦРУ, который, как выяснилось, работал с 1985 г. на СССР, а затем, до ареста в 1994 г., – на Россию, выдал сотни агентурных операций ЦРУ, РУМО и ФБР, в результате чего, по меньшей мере, 10 граждан Советского Союза и стран Восточной Европы были казнены, другие посажены в тюрьму, а агентурная сеть, развернутая США против советского блока, была фактически полностью ликвидирована еще в разгар «холодной войны» [Ibid.]. В 2001 г. был арестован Роберт Хансен – сотрудник ФБР, в течение двух десятилетий работавший на советскую, а затем российскую разведку и выдавший секретные программы и разведывательные возможности, которые стоили правительству США 22 млрд долл. [11, p. 1] и могли бы быть использованы так, чтобы в случае войны уверенно нанести поражение США. Наконец, Ана Монтес, аналитик Разведывательного управления министерства обороны США, выдала за 15, а по некоторым утверждениям 17 лет работы на кубинскую разведку всю разведывательную программу США против Кубы, как электронную, так и агентурную [Ibid.].

Среди стран, направлявших своих агентов в США, пальма первенства принадлежит СССР и России. Половина из 247 человек, арестованных за шпионаж в Соединенных Штатах с 1945 по 2008 г. (49 % или 121 человек), была связана с Советским Союзом или Россией. Д. Мэйджор отмечал, что «контрразведывательное сообщество США осваивало искусство контрразведки, изучая операции КГБ и ГРУ по всему миру» [6, p. 2]. Озабоченность по поводу деятельности российской разведки сохранилась и после окончания «холодной войны». «Служба внешней разведки новой демократической России – Служба внешней разведки России (СВРР) продолжает работать против нас. Это СВРР приняла кураторство над Олдричем Эймсом от своего предшественника, КГБ, в 1991 г. Это СВРР направляла деятельность сотрудника ЦРУ Гарольда Джеймса Николсона против нас в 1994–1996 годах. Это СВРР управляла специальным агентом ФБР Ёарлом Питсом, когда он был арестован за шпионаж в 1996 г. Это СВРР установила подслушивающее устройство в конференц-зале Государственного департамента в Вашингтоне летом 1999 г. И это СВРР управляла специальным агентом ФБР Робертом Хансеном, когда он был арестован по обвинению в шпионаже в феврале 2001 г.», – с раздражением и тревогой констатировал ветеран американской контрразведки Джеймс М. Олсон [9, p. 1]. Нашумевшее дело «русских нелегалов» 2010 г. предоставило новую возможность говорить о серьезности угрозы шпионажа против США иностранных держав, которые «конкурируют с Соединенными Штатами в экономической, военной и дипломатической сферах». Пример ареста сети из 10 русских шпионов позволил директору ФБР заявлять о существовании «долгосрочных планов наших противников», а о масштабах и характере угроз должны были свидетельствовать детали последнего дела. «Направленные сюда в течение двух последних десятилетий русские агенты приобрели облик средних американцев, во многих случаях используя лживые “легенды” граждан Соединенных Штатов, имели работу и вели тихую семейную жизнь. Эти агенты получали сотни тысяч долларов наличными от своих кураторов для обеспечения секретности в Америке, поддерживая связь при помощи радио и Интернета», – делился подробностями директор ФБР [7].

Естественно, что во времена «холодной войны» американская контрразведка концентрировала свое внимание на советской разведке и разведслужбах стран советского блока. Однако, когда в начале 1990-х гг. ФБР стало смотреть шире и инициировало расследования в отношении всех стран, которые собирали развединформацию о США, оно обнаружило более сотни таких государств. При этом 28 стран были публично идентифицированы как вовлеченные в проведение шпионских операций против США [6, p. 2–3]. В последнее время возрастает озабоченность американской контрразведки по поводу усиления китайского шпионажа в США. Директор ФБР Р. Мюллер даже определил шпионаж со стороны Китая как наиболее серьезную угрозу со стороны иностранных разведок. Один из последних эпизодов, связанных с КНР, – дело Чи Мака, осужденного в 2007 г. федеральным судом Калифорнии за шпионаж, имевший серьезные последствия для вооруженных сил США. Он выдал информацию о радаре для корабля ВМФ следующего поколения. Чи Мак был не государственным

служащим, а сотрудником подрядной организации, который работал над проблемой минимизации шумов американских подводных лодок и надводных кораблей. «Разработка технологий, которые он выдал, стоила американским налогоплательщикам миллиарды долларов, а китайцы получили их бесплатно. То, что он сделал, сократило на годы технологическое преимущество ВМФ США. Это ослабило сдерживающие возможности в Тайваньском проливе. И это подвергло риску жизни наших сыновей, дочерей и соотечественников в ВМФ», – отмечал Дж. Бреннер [2, p. 4]. В целом, шеф контрразведки ФБР Дэйв Зэйди констатировал в 2006 г., что угроза со стороны иностранных шпионов сейчас «серьезней, чем была во время холодной войны» [4].

ФБР, проведя в начале XXI века всеобъемлющую оценку угроз со стороны нескольких стран, вызывающих особую озабоченность контрразведки, определило пять категорий иностранной разведывательной деятельности, особенно вредоносной для национальной безопасности США, и расставило их в следующем порядке по степени важности: 1) распространение информации и технологий, связанных с производством химического, бактериологического, радиологического, ядерного оружия и высокомощных взрывчатых веществ; 2) проникновение в разведывательное сообщество США; 3) проникновение в организации правительства США и его подрядчиков; 4) рассекречивание важных национальных ресурсов – политических проектов, планов, технологий, производственных процессов и иной информации – которые, в случае их похищения, модификации или использования противником, серьезно угрожали бы национальной или экономической безопасности США; 5) осуществление тайной иностранной разведывательной деятельности в США.

Кроме того, ФБР выделило три категории субъектов иностранной разведывательной деятельности на территории США: 1) страны, которые традиционно считают США своей главной разведывательной целью, противником или угрозой, что проявляется в сохранении их широкого и активного разведывательного присутствия в США и в их агрессивной атаке на американских граждан, информацию и технологии; 2) страны, которые, не обязательно рассматривают США как противника или угрозу, но ищут информацию, которая помогла бы им в международной экономической, военной и политической конкуренции (и США как лидер во всех этих трех сферах становятся их главной мишенью); 3) страны, для которых США представляют не столько разведывательную цель, сколько оперативную среду для осуществления разведывательной деятельности, сфокусированной на их внутренней безопасности.

Директор ФБР Р. Мюллер отмечал, что некоторые страны становятся все более осведомленными, подготовленными и оснащенными в противоборстве с контрразведкой. Все большую озабоченность вызывает асимметричная угроза со стороны некоторых разведывательных служб, которые используют «нетрадиционных агентов»: студентов, членов делегаций, командированных, эмигрантов и отставных разведчиков, осуществляющих сбор развединформации по мере возможности или в соответствии с отдельными запросами разведывательных служб. При этом подчеркивается, что такие нетрадиционные охотники за информацией представляют потенциальную угрозу на всей территории США, что требует скоординированного ответа со стороны всех местных отделов ФБР. Более того, ФБР отмечает, что некоторые страны используют своих офицеров связи, которые находятся в США с миссией обмена разведывательными данными, для сбора чувствительной оборонной информации, находящейся за пределами официально разрешенного доступа. Директор ФБР признавал, что наиболее трудно поддается выявлению и оценке деятельность по сбору развединформации, направляемая и (или) осуществляемая непрофильными организациями, такими как неразведывательные ведомства иностранных правительств и (или) иностранные компании. Этот тип деятельности чаще всего отмечался ФБР в области поиска и добывания информации и технологий, связанных с производством химического, бактериологического, радиологического, ядерного оружия и высокомощных взрывчатых веществ.

Еще один вызов, с точки зрения ФБР, представляют попытки некоторых иностранных разведок использовать международные межведомственные связи в целях сбора разведданных. Директор ФБР докладывал на слушаниях в сенате, что граждане США, участвующие в международных конференциях и программах обменов, или те, в чьи обязанности входят рутинные контакты с представителями иностранных разведок, часто сообщают, что коллеги, с которыми они контактируют, пытаются вытягивать из них различные сведения подчас настолько агрессивно, что это вызывает удивление.

ФБР прогнозировало, что в ближайшей перспективе приоритетными целями в сборе информации о Соединенных Штатах будут следующие: влияние выборов в США на внешнюю и внутреннюю политику страны, военные действия США в Ираке и Афганистане, контртеррористическая политика США, технологии двойного применения, политика США в отношении конкретных стран и регионов мира. ФБР также ожидало увидеть продолжение влияния со стороны иностранных разведслужб на формирование восприятия тех или иных процессов и событий. Наконец, ФБР предполагало, что многие иностранные разведывательные службы продолжат использовать свое присутствие в США для того, чтобы работать и собирать информацию против третьих стран, а также заниматься «оборонительной разведывательной деятельностью», целью которой будут их собственные соотечественники и этнические сообщества в США, особенно те группы, которые рассматриваются как угроза существующим режимам [8].

Однако угроза шпионажа может исходить не только со стороны иностранных держав и их спецслужб. В официальных оценках разведывательных угроз Соединенным Штатам после 11 сентября 2001 г. к государствам, собирающим развединформацию о США, добавились террористические организации, обычно предваряющие свои атаки разведывательными мероприятиями. По утверждению Мишель Ван Клив, руководителя национальной контрразведки США в 2003–2006 гг., 35 установленных или подозреваемых террористических организаций собирают разведывательную информацию о США агентурным путем или другими методами [11, p. 2]. Цели организаций, ведущих разведку против США, по оценке американской контрразведки, разнообразны и широки. Среди них отмечается, например, стремление украсть секреты национальной безопасности Соединенных Штатов, чтобы использовать их в военных или террористических целях. Делается акцент и на попытках иностранных сторон ослабить США во внешней политике (торговле) или использовать в своих интересах то, что они узнали об американских разведывательных возможностях, чтобы скрывать свои действия или направить американские службы по ложному следу. Как резюмировала М. Ван Клив, «если оставить [эти попытки] без ответа, их успех мог бы нам дорого стоить, поставив под угрозу операции США, военный и разведывательный персонал и американских граждан на территории страны» [Ibid.].

По мнению американских аналитиков, за последние годы произошло и продолжается расширение круга контрразведывательных угроз. Помимо традиционного шпионажа, в отношении военных секретов все большее значение приобретает экономический и научно-технический шпионаж, в котором, в свою очередь, происходят изменения, связанные с научно-техническим прогрессом. Охота за технологиями и экономическими секретами США воспринимается руководством американской контрразведки как одна из главных угроз, так как ослабляет США в разных отношениях – экономическом, военном, политическом, лишает преимуществ США и дает даром или дешево другим то, за что США дорого заплатили. Значительно возросли возможности сбыта украденных технологий и, соответственно, экономическая привлекательность этого «бизнеса». «Мы живем в мире, в котором Соединенные Штаты не могут более полагать, что имеют качественное технологическое превосходство над друзьями и противниками. Мир стал более плоским, значительно более плоским. Более того, грязный мир украденной информации стал все более экономически рациональным, – рассуждал Дж. Бреннер. – Воры, неспособные использовать информацию, но знающие, как ее украсть, сейчас поняли, как ее продавать. Развернулся широкий рынок для секретов, а среди продавцов на этом рынке – хакеры-любители, преступные группировки и иностранные разведывательные службы» [1, p. 2].

Американские контрразведчики объясняют широкие масштабы деятельности иностранных разведок в США не только интересом к секретам и технологиям передовой державы, но и особенностями американского общества: «Наша общая культура открытости предоставляет иностранным организациям легкий доступ к совершенным технологиям. Каждый год, например, мы впускаем в США десятки тысяч иностранных посетителей на объекты, связанные с государством, такие как военные базы, испытательные центры, исследовательские лаборатории. Некоторые из этих посетителей занимаются приобретением американских технологий и ноу-хау, которые иначе недоступны» [11, p. 3]. В частности, они указывали на то, что американские колледжи и университеты, центры разработки высоких технологий принимают на работу большое число преподавателей и сотрудников иностранного

происхождения и обучают большое число иностранных студентов, многие из которых вернутся в свои страны. Например, все возрастающее число и доля преподавателей естественных и технических факультетов университетов и колледжей США, приближающееся к 30 %, – иностранцы по происхождению. Более того, около 40 % докторских степеней, присуждаемых университетами США по техническим и инженерным наукам (приблизительно 8000 в год), приходятся на иностранных студентов. «Большинство этих студентов законно учатся и преследуют академические цели. Но не все», – отмечала М. Ван Клив [Ibid. p. 4].

Аналитики в США обращают внимание на стремительное развитие информационных технологий, которое в то же время расширяет и упрощает нелегальное изъятие, хранение и передачу огромных массивов данных, включая торговые секреты и патентную информацию. Изощренные информационные системы, которые создают, хранят, обрабатывают и передают секретные сведения, становятся все более уязвимыми для нелегального использования. Многие страны имеют специальные программы для сбора информации, находящейся в компьютерных сетях, и зарубежные конкуренты разрабатывают способы, позволяющие использовать эти уязвимые места. Глобализация перемешала иностранные и американские кампании таким образом, что затруднила защиту технологий, которые эти фирмы разрабатывают или приобретают, когда эти технологии предназначены для использования за рубежом [Ibid.]. При таком доступе, который иностранцы имеют к американским технологиям, и важности последних для экономического и военного развития, не должно удивлять то, что люди из многих стран вовлечены в их «креативное приобретение». Только в 2004 г. контрразведывательное сообщество зафиксировало попытки приобрести секретные технологии США бизнесменами, учеными, университетскими преподавателями и студентами почти из 100 государств мира. Правда, несмотря на длинный список, значительная часть подобной активности приходится на небольшое число людей из ограниченного числа мест. Например, согласно Службе безопасности министерства обороны, в 2004 г. 60 % подозрительных усилий по сбору сведений у подрядчиков министерства обороны, имеющих допуск к секретам, приходилось на 10 государств, наиболее активных, с точки зрения американской контрразведки. Эта первая десятка – неоднородная группа. В нее входят противники и союзники США, богатые и бедные страны. Но два государства всегда находятся в начале списка – это Китай и Россия [Ibid. p. 4–5].

М. Ван Клив признавала существование значительных разведывательных пробелов в понимании того, как иностранные государства занимаются добыванием информации об американских технологиях. Но некоторые вещи, связанные с промышленным шпионажем, спонсируемым государствами, она называла со всей уверенностью. В частности, она отмечала, что ряд ведущих иностранных разведок имеют программы приобретения технологий при помощи подставных фирм; списки искомых технологий и специальные стратегии их приобретения; соглашения об обмене технологиями, законно и незаконно приобретенными, с разведывательными службами других стран. При охоте за чувствительными технологиями используется широкий спектр методов, далеко выходящих за рамки тех приемов, которые традиционно ассоциируются со шпионажем. Чаще всего используются наиболее простые, дешевые и наименее рискованные способы. Например, в большинстве случаев информация или технологии просто запрашиваются по электронной почте, телефону, факсу, письмом или при личной встрече. Когда авторы запроса получают отказ или предложение обратиться за экспортной лицензией, они прекращают коммуникации и ищут другого потенциального поставщика, пока не найдут фирму, не знающую требований по лицензированию экспорта либо игнорирующую их. Другим распространенным методом являются визиты на фирмы, военные базы, в национальные лаборатории и к частным поставщикам министерства обороны. Считается, что особую опасность могут представлять иностранные визитеры, прибывшие на долгий срок. Каналом утечки американских технологий могут служить иностранные студенты, ученые и другие эксперты, прибывающие в США на работу или для участия в конференциях. Американские бизнесмены, выезжающие за рубеж, также рассматриваются как мишень для иностранных разведок, тайно снимающих информацию с ноутбуков, PDA и мобильных телефонов [Ibid. p. 7].

Перспективы экономического шпионажа против США, по прогнозам американской контрразведки, тревожные. «Мы не должны ожидать снижения иностранного спроса на чувствительные технологии США в ближайшие годы… В то же время задача сокращения незаконного оттока

технологий будет становиться все трудней. Глобализация, которая приносит Соединенным Штатам экономическую выгоду, делает все более сложной сохранение экономических секретов от иностранных менеджеров и персонала. Все больше американские фирмы осуществляют НИОКР в центрах, расположенных вне границ США, где будет трудно обеспечивать физическую безопасность, а правовая защита технологий, экономических секретов и инноваций будет слабой или ее не будет вообще», – предупреждала М. Ван Клив [Ibid. p. 9]. Растущую озабоченность у американских спецслужб вызывают проблемы, связанные с использованием иностранными разведками современных информационных технологий для получения секретной информации США, «угроза со стороны инсайдера – человека, имеющего доступ к компьютерной системе американской фирмы, но на самом деле работающего на иностранную организацию» [Ibid.].

Дж. Бреннер, сменивший М. Ван Клив на посту руководителя национальной контрразведки в 2006 г., продолжил эту тему, но внес в нее новые элементы. В частности, явный акцент был сделан на угрозы кибернетическому пространству США и проблемы его контрразведывательной защиты. Он утверждал, что «работа не становится легче. Существует около 140 иностранных разведывательных служб, чья главная цель – Соединенные Штаты и американские кампании. Но она не становится легче еще и по другой причине. Сегодня информация – это электроны. Электроны двигаются по киберсетям, а эти сети уязвимы» [2, p. 3].

Отмечая изменения в структуре контрразведывательных угроз Соединенным Штатам, Дж. Бреннер выделил две новых проблемы: уязвимость компьютерных сетей и риски, связанные с приобретением информационно-коммуникационного оборудования на рынке, который становится все более интернационализированным [1, p. 7]. Говоря о первой проблеме, Дж. Бреннер отмечал, что «электронные сети страны слишком легко взломать, а количество хакеров мирового класса растет с головокружительной быстротой. Понятно почему: если вы можете извлечь большие объемы информации электронным путем, находясь в комфортабельном офисе на другом континенте, зачем идти на расходы и риск, связанные с использованием разведчика или проведением разведывательной операции? Если можно вывести из строя важную инфраструктуру электронным путем с другого конца света, зачем нужен местный диверсант?» [3, p. 2] «Уязвимость кибер-сетей – новый рубеж для контрразведки», – заявлял Дж. Бреннер и подчеркивал, что «эта проблема – стратегическая», поскольку «министерство обороны одно не может справиться с ней. Разведывательное сообщество, действуя в одиночку, также не сможет справиться с ней. Правоохранительные органы все еще борются с мелкими хакерами, не обращая внимания на угрозу, о которой я говорю» [Ibid. p. 4].

Поясняя новизну проблемы для контрразведки и безопасности, Дж. Бреннер утверждал: «Кибернетический вызов выходит за пределы старой парадигмы безопасности: на него не ответишь тем, что сделаешь покрепче замок для более крепкого ящика, в котором хранятся секреты. Единственный способ полностью устранить риск взлома или поражения сетей – прекратить коммуникации и отключиться. Но мы не собираемся делать это» [Ibid.] В этом вызове Дж. Бреннер выделил «три связанных, но разных проблемы: уязвимость оборудования, уязвимость программного обеспечения и человеческое поведение», отметив, что труднее всего справиться с последней. «Мы, американцы, любим наши удобства, мы привыкли к быстрому удовлетворению наших потребностей. Мы усовершенствовали нашу технику, чтобы делать многие вещи легче, дешевле и быстрее, но наше нетерпение часто бывает нашей ахиллесовой пятой… Когда удобство сталкивается с безопасностью, удобство всегда побеждает. А если вы добавите в эту смесь глупость, злонамеренность и беспечность, а я боюсь, мы найдем эти качества в той или иной мере в любой организации – государственной или частной – вы получите предпосылки серьезных проблем в информационно-компьютерных сетях» [1, p. 4].

Второй контрразведывательный риск – «проблема приобретения». Она связана с тем, что частные фирмы и правительственные организации, включая разведывательные агентства, покупают коммуникационное и другое оборудование на открытом международном рынке. «Что мы покупаем? Что значит “сделано в США”, когда комплектующие компоненты поступают из-за границы, а программное обеспечение может быть написано бог знает кем? Неизвестное или сомнительное происхождение повышает риск того, что иностранное правительство или организация могут запрограммировать уязвимость наших самых важных информационных систем» [3, p. 2].

Подобный анализ угроз логически приводит к коррекции понятия контрразведки и его расширительному толкованию. Дж. Бреннер отмечал: в

условиях глобализации, ставшей фактом жизни в XXI столетии, «под контрразведкой я понимаю нечто более широкое, чем борьбу с традиционным шпионажем против правительств. Сегодня контрразведка больше не является сугубо правительственной проблемой. Это проблема для любой фирмы, имеющей секреты, независимо от того, могут они быть официально засекречены или нет. И это проблема любого предприятия, которое использует электронные устройства для коммуникаций, то есть постоянная проблема всех предприятий в течение всего времени» [Ibid. p. 1–2].

Помимо внешних влияний, по оценке американских специалистов, целый ряд внутренних факторов, действующих в последние десятилетия, усиливает риск шпионажа против США со стороны собственных граждан. Авторы военного центра по изучению проблем безопасности в Монтерее (Калифорния) делят их на две части: 1) возможности и 2) мотивы для ведения инсайдерского (внутреннего, то есть силами самих американских граждан) шпионажа. И те и другие, по мнению экспертов, в последние десятилетия усиливаются и, взаимодействуя, создают среду, таящую возрастающий риск для безопасности США. Для парирования этого риска предлагается действовать по трем направлениям: совершенствовать работу по проверке персонала, усилить защиту информации и активизировать деятельность контрразведки, обеспечив согласованность усилий на всех направлениях [5].

Таким образом, основные выводы, которые следуют из анализа американской контрразведкой шпионажа против США, состоят в том, что он не только не исчез, но, напротив, видоизменяясь, приобретает еще большую опасность в условиях глобализации и войны с терроризмом. При этом формируется широкое и цельное понимание этой угрозы не как специфической проблемы отдельных государственных органов или частных фирм, имеющих секреты, но как общенационального стратегического вызова. Подобные оценки отражаются на разных аспектах американской контрразведки – организационной структуре и системе управления, стратегии и тактике, формах и методах работы, и, таким образом, в целом воздействуют на эволюцию контрразведывательного сообщества США.

Библиографический список

1. Brenner, Joel F. “Counterintelligence in the 21st Century: Not Just a Government Problem”. Remarks at the AFCEA Counterintelligence Conference, Sunnyvale, CA. December 4, 2007. [electronic resource] : http://www. ncix. gov/publications/speeches/AFCEASpeech. pdf (10.11.2008)

2. Brenner, Joel F. “Intelligence, Thinking, and Academia”. Remarks at the Intelligence Community Centers of Academic Excellence Summer Seminar. 24 July, 2007. [electronic resource] : http://www. ncix. gov/publications/speeches/SummerSeminar. pdf (08.11.2008)

3. Brenner, Joel F. “Strategic Counterintelligence: Protecting America in the 21st Century”. Remarks at The Nro/National Military Intelligence Association Counterintelligence Symposium. Washington, DC. 24 October 2007. [electronic resource] : http://www. ncix. gov/publications/speeches/NNMIASpeech. pdf (10.11.2008)

4. Gertz, Bill. Counterintelligence posts vacant // The Washington Times. – February 10, 2006. [electronic resource] : http://www. washingtontimes. com/national/20060210-123648-8710r. htm (03.01.2009)

5. Kramer, Lisa A. and Richards J. Heuer Jr. America’s Increased Vulnerability to Insider Espionage // International Journal of Intelligence and CounterIntelligence. – Volume 20. – Number 1. – 2007. – Pp. 50–64.

6. Major, David G. “Enforcement of Federal Espionage Laws”. Prepared Statement Before the US House of Representatives, Committee on the Judiciary, Subcommittee on Crime, Terrorism, and Homeland Security. January 29, 2008. [electronic resource] : http://www. fas. org/irp/congress/2008_hr/012908major. pdf (20.02.2009)

7. Mueller, Robert S. Statement before the Senate Judiciary Committee. Washington, D. C. July 28, 2010. [electronic resource] : http://www. fbi. gov/news/testimony/fbi-priorities-successes-and-challenges (08.10.2010)

8. Mueller, Robert S. Testimony before the Senate Committee on Intelligence of the United States Senate. February 16, 2005. [electronic resource] : http://www. fbi. gov/congress/congress05/mueller021605. htm (08.01.2009)

9. Olson, James M. A Never-Ending Necessity. The 10 Commandments of Counterintelligence // Studies in Intelligence. – Fall-Winter 2001. – No. 11 [electronic resource] : http://www. ncix. gov/archives/docs/10CommandmentsofCI_cind-2002-01-05. pdf (12.07.2008)

10. Threat Assessment [electronic resource] : http://www. centerforintelligencestudies. org/ThreatAssessment. html (24.09.2010)

11. Van Cleave, Michelle. Statement before the House Judiciary Subcommittee on Immigration, Border Security & Claims. Hearing on Sources and Methods of Foreign Nationals Engaged in Economic and Military Espionage. September 15, 2005. [electronic resource] : http://www. ncix. gov/publications/reports_speeches/speeches/JudiciaryDraftBriefing050913a_final. pdf (18.03.2009)