ПОНЯТИЕ И СОДЕРЖАНИЕ СИСТЕМЫ СОБИРАНИЯ И АНАЛИЗА ДАННЫХ, ПОЛУЧЕННЫХ ИЗ ОТКРЫТЫХ ИСТОЧНИКОВ, В РАЗВЕДЫВАТЕЛЬНОМ СООБЩЕСТВЕ США (OSINT)

Ю.С. Петухов (Витебск)

Современные международные отношения характеризуются нарастанием конкурентного противоборства между ведущими странами мира в целях достижения геополитического доминирования. Важнейшую роль в этом противоборстве играют США, ведомые идеей всемирного лидерства и готовые достичь его, в том числе и с использованием силовых методов. В этих условиях одно из ключевых мест в стратегии и тактике их внешней политики принадлежит разведывательной деятельности как средству информирования органов государственного и военного управления и содействия принятию целесообразных и своевременных решений.

Структура разведывательной деятельности спецслужб США претерпела значительные изменения со времен геополитического противостояния с СССР. В начале 1990-х гг. появился Интернет – всемирная система объединённых компьютерных сетей, которые образуют информационное пространство, представляющее собой совокупность динамично обновляющихся данных. По своей природе Интернет стал неисчерпаемым источником данных любой тематики, и в настоящее время ни один вид социальной деятельности, включая и разведывательную, невозможен без систематического анализа информации, распространяемой в глобальной сети. Разведывательное сообщество США (РС США) успешно освоило предоставленный Интернет информационный потенциал, что нашло выражение в выделении в его методологии особого вида разведывательной деятельности, получившего название OSINT (opensourceintelligence – рус. «разведка на основе открытых источников информации») и формулировке его специфических целей, задач, методов, принципов. В американской традиции принято говорить об OSINT как разведывательной дисциплине, однако в рамках отечественной методологии целесообразно рассматривать ее как *систему собирания и анализа разведывательных данных.*

В настоящее время не существует единого подхода к определению семантического объема OSINT как термина. К примеру, Е. Бен Бенавидес понимает под OSINT«разведывательную дисциплину, которая включает информацию, собираемую из открытых источников, и ее анализ для производства пригодных к работе разведданных при отсутствии необходимости их засекречивания для эффективного использования» [1, с. 8]. К. Берд полагает, что «термином OSINT обозначают сбор и анализ разведданных на основе информации из общедоступных источников» [2]. Дэйв Маркус, директор McAfeeLabs, считает, что под OSINT следует по-

нимать «форму управленческой деятельности по собиранию данных, которая включает обнаружение, отбор, приобретение информации из публично доступных источников и ее анализ с целью получения выводных разведданных» [3].

Однако в качестве основного целесообразно принимать нормативное определение, закрепленное в законодательстве США. Так в Законе «О национальной обороне в 2006 бюджетном году» изложено следующее определение OSINT: «ценная разведывательная дисциплина, которая должна быть включена в менеджмент разведывательных задач, собирание, обработку, использование и распространение разведданных с целью гарантии полного и своевременного информирования высших чиновников Соединенных Штатов» [4, sec. 931, §A, п. 3]. Эта дефиниция, построенная с использованием форм будущего времени, на момент ее принятия не являлась окончательной, однако в нормативных актах США более поздних определений OSINT не обнаружено.

Принимая во внимание, что информирование государственных органов и должностных лиц является непосредственной задачей любой спецслужбы, следует полагать, что в структуре РС США OSINT понимается как *система собирания и анализа разведданных, включающая менеджмент задач разведки, собирание, обработку, использование и распространение к целевой аудитории информации, полученной из открытых источников, и осуществляемая уполномоченными государственными органами в целях решения возложенных на них задач.*

OSINT, как система собирания и анализа разведывательных данныхРС США, характеризуется специфическими признаками: 1. Оперирование общедоступной несекретной информацией. Поскольку в качестве объекта OSINT выступают сведения, не отнесенные к государственным секретам США или других стран, то аналитики РС не сталкиваются с препятствиями по их получению, а также не ограничены режимными мерами при организации работы с ними и передаче союзникам США; 2. Осуществление уполномоченными на то органами. В настоящее время число органов, осуществляющих OSINT как систему собирания и анализа разведданных, не ограничивается основным перечнем субъектов РС США, поскольку включает также подведомственные им подразделения; 3. Осуществление в целях решения разведывательных задач. Реализация возможностей OSINT в рамках деятельности уполномоченных на ее проведение органов лежит в русле решения острых тактических вопросов и построения стратегических прогнозов деятельности американской разведки или воинских контингентов, выполняющих задачи за рубежом; 4. Наличие методологически установленной процедуры осуществления OSINT, включающей менеджмент разведывательных задач, собирание, обработку, использование и распространение информации к целевой аудитории и составляющей, таким образом, содержание OSINT как системы собирания и анализа разведданных. Следовательно, могут быть выделены и описаны основные компоненты содержания OSINT:

1. Менеджмент задач разведки (intelligencetasking, intelligence planning and direction). Заключается в формулировании разведывательных запросов к подразделению, осуществляющему OSINT, а также в организации «обратной связи» (feedback), призванной информировать аналитические подразделения о степени соответствия представленной ими выводной разведывательной информации изначальным запросам [5, с. 16 – 17].

2. Собирание (collection). Представляет собой процесс поиска открытой информации и получения права на владение либо доступ к ней. Под поиском понимается соотнесение разведывательного запроса с доступными источниками информации в целях создания аналитического продукта, удовлетворяющего этот за-

прос [5, с. 17]. После определения круга адекватных запросу источников происходит собственно собирание информации. Стоит отметить, что в Директиве РС США № 301 от 11.07.2006 г. в качестве синонимичных рассматриваются два термина – собирание (collection) и приобретение (acquisition), причем в качестве предпочтительного указывается последний, так как «по определению, открытые источники накапливают и распространяют открытую информацию, предварительно собранную другими пользователями. Таким образом, аналитики разведки получают ее как бы из вторых рук»[6, §F, п. 1]. Логика данного суждения состоит в том, что собранная и распространенная кем-либо информация изначально уже имеет своего правообладателя, поэтому методологически верно говорить именно о приобретении открытых данных, хотя бы и безвозмездном.

3. Обработка и использование (processin gand exploitation). Под обработкой понимается применение к первичным данным, полученным путем собирания, методов и приемов аналитической деятельности с целью проверки релевантности источника и достоверности полученных из него сведений. Следующим этапом является использование, то есть приведение полученной выводной развединформации в соответствие с формальными требованиями заказчика (перевод, оформление в виде документа и т.д.) [5, с. 23 – 24].

4. Распространение к целевой аудитории (dissemination). Состоит в предоставлении заказчику выводной разведывательной информации [5, с. 33]. При этом следует отметить, что ввиду несекретного характера разведданных OSINT в перечень их получателей включены не только субъекты РС США, но и органы государственной власти и управления, политические структуры, негосударственные организации. К примеру, регистрация на официальном сайте National OpenSource Center предоставляется всем государственным служащим США федерального, регионального и местного уровней в целях получения доступа к полному объему разведданных OSINT по более чем 160 странам на 80 языках [7].

Обратив внимание на структуру содержания OSINT как системы собирания и анализа разведданных, можно сделать вывод о существовании определенного алгоритма ее осуществления спецслужбами США, который, по нашему мнению, может быть назван, *разведывательным циклом OSINT*. Одновременно следует выделить основные факторы уязвимости национальной безопасности разведываемых государств перед возможностями «открытой разведки»:

1. Незащищенность открытых данных. По своей природе информация, содержащаяся в Интернет, доступна всем пользователям сети, что устраняет перед разведкой препятствия к работе с ней.

2. Низкие возможности противодействия OSINT. Данная деятельность осуществляется с территории своего государства, а потому практически полностью безопасна [2].

3. Оперативность решения разведывательных задач. По нормам стран НАТО предоставление выводных данных осуществляется в течение 4 часов после поступления запроса в подразделение, осуществляющее OSINT [5, с. 19].

4. Рационализация использования сил и средств разведки. Стратегии OSINT не являются ресурсоемкими, и разведка может перераспределить свои усилия более эффективным образом.

Исходя из вышеизложенного, следует полагать, что в распоряжении РС США находится действенный правовой и организационный механизм использования открытых источников информации в целях решения разведывательных задач. При надлежащей организации работы, достаточном финансировании и материально-техническом обеспечении, а также привлечении к осуществлению дан-

ной деятельности квалифицированных аналитиков и программистов, он способен эффективно реализовать разведывательный потенциал открытой информации и создать РС США стратегическое превосходство перед разведывательными органами других субъектов международных отношений.

1. Ben Benavides, E. Open Source Intelligence (OSINT) Link Directory: Targeting Tomorrow's Terrorist Today (T4) through OSINT / E. Ben Benavides // AGM: AllSource Global Management [Electronic resource]. –Mode of access: http://www.agm-az.com/docs/Benavides%20Online%20OSINT%20Quick%20Reference%20Handbook%20New%20Table%20of%20Contents.pdf. – Date of access: 13.07.2012.
2. Берд, К. Модель OSINT / К. Берд // Новости конкурентной разведки [Электронный ресурс]. – Режим доступа: http://analitirus.blogspot.com/2012/01/osint.html. – Дата доступа: 30.06.2012.
3. Marcus, D. Emerging Threats and Trends. How To Social Engineer With 100% Success Using OSINT / D. Marcus // US-CERT: United States Computer Emergency Readiness Team [Electronic resource]. –Mode of access: http://www.us-cert.gov/GFIRST/presentations/Emerging_Trends_in_2010.pdf. – Date of access: 17.08.2012.
4. National Defense Authorization Act for Fiscal Year 2006. Public Law 109–163, 109th Congress // GPO: Government Printing Office [Electronic resource]. –Mode of access: http://www.gpo.gov/fdsys/pkg/PLAW-109publ163/html/PLAW-109publ163.htm. – Date of access: 06.10.2012.
5. NATO Open Source Intelligence Handbook, November 2001 // The Air University [Electronic resource]. – Mode of access: http://www.au.af.mil/au/awc/awcgate/nato/osint_hdbk.pdf. – Date of access: 29.06.2012.
6. Intelligence Community Directive № 301, July 11, 2006// Federation of American Scientists [Electronic resource]. – Mode of access: www.fas.org›irp/dni/icd/icd-301.pdf. – Date of access: 17.08.2012.
7. Open Source Center Information to Intelligence [Electronic Resource]. – Mode of access: http://www.opensource.gov. – Date of access: 20.08.2012.