ISSN 2311-875X (Online)
ISSN 2073-2872 (Print)

Угрозы и безопасность

НАЦИОНАЛЬНЫЕ ИНТЕРЕСЫ – АКТУАЛЬНЫЕ ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ ИСПОЛЬЗОВАНИЮ ИНТЕРНЕТА ТЕРРОРИСТИЧЕСКИМИ И ЭКСТРЕМИСТСКИМИ ОРГАНИЗАЦИЯМИ

Андрей Анатольевич МАЙДЫКОВ[a,*], Олег Борисович ИСАРОВ[b]

[a] кандидат юридических наук, доцент, ведущий научный сотрудник, НИЦ № 2 ВНИИ МВД РФ, Москва, Российская Федерация
maydikov@mail.ru

[b] кандидат юридических наук, ведущий научный сотрудник, НИЦ № 2 ВНИИ МВД РФ, Москва, Российская Федерация
07070@lenta.ru

[*] Ответственный автор

История статьи:
Принята 28.04.2015
Одобрена 20.05.2015

УДК 343.143
JEL: P37

Ключевые слова: интернет-ресурсы, социальная сеть, информационные сети, терроризм, экстремизм

Аннотация

Тема. В статье дана общая оценка состояния использования Интернета террористическими и экстремистскими организациями. Рассмотрены основные направления работы по минимизации экстремистско-террористических проявлений в социальных сетях.

Задачи. Авторами предпринята попытка решения ряда важных правовых, организационных и иных задач, связанных с повышением эффективности преодоления проблем противодействия использованию Интернета террористическими и экстремистскими организациями.

Методология. Предложенный методологический подход состоит в определении основного направления противодействия использованию Интернета террористическими и экстремистскими организациями в соответствии с установленными приоритетами государственной политики.

Результаты. Разработаны структура и порядок действий по определению основных характеристик использования Интернета террористическими и экстремистскими организациями, статуса и функциональных возможностей лиц, намеревающихся совершить террористические и экстремистские действия с использованием глобальной сети. Дана общая оценка ситуации в данной сфере, предложены способы построения эффективной работы по своевременному выявлению, раскрытию и профилактике терроризма и экстремизма. Приведены конкретные рекомендации по решению проблем безопасности при организации противодействия использования Интернета террористическими и экстремистскими организациями.

Применение. Результаты проведенного исследования позволят осуществлять государственное планирование, определять порядок и способы реализации целей и задач развития правоохранительной национальной стратегии в данном направлении.

Выводы. Предложенный метод программно-целевого анализа основных способов использования Интернета террористическими и экстремистскими организациями должен стать государственным инструментом для проведения адресной и эффективной работы по профилактике и раскрытию преступлений в данной сфере. Он необходим для управления и контроля за реализацией планов и программ национальной безопасности России, строительства и развития профильных правоохранительных структур, внедрения новых методик и правовых инструментариев.

Возникновение сети Интернет восходит к началу 1970-х гг., периоду обострения холодной войны между социалистической и капиталистической политическими системами, когда министерство обороны США всерьез обеспокоилось уязвимостью его сетей в связи с возможностью ядерной атаки. Американцы пришли к необходимости децентрализации своих центров данных за счет создания связанных между собой участков компьютерных сетей.

После 20 лет развития и использования его возможностей в научных исследованиях к концу 1980-х гг. характер сети Интернет начал меняться в силу предоставления доступа в него коммерческим пользователям. К середине 1990-х гг. Интернет объединял в себе более 18 000 частных, общественных и национальных сетей, количество его пользователей год от года стремительно росло. На сегодняшний день в глобальной сети представлены более 3,2 млн хостов и 60 млн активных пользователей со

всех континентов планеты. Предполагаемое число клиентов Интернета в настоящее время составляет более миллиарда человек [1–6].

В современном мире практически все действующие в различных регионах террористические группы так или иначе обнаруживают свое присутствие в Интернете. В результате исследования, проведенного израильским социологом Г. Вайнманом еще в 2003–2004 гг., в глобальной сети были обнаружены сотни веб-сайтов подобных групп и их сторонников. К сожалению, к настоящему моменту ситуация серьезно усугубилась. К опасным террористическим организациям (ТО), активно использующим сегодня ресурсы Интернета, можно отнести: ХАМАС (Движение исламского сопротивления, международная ТО); «Хезболла» («Партия Аллаха», международная ТО); «Аль-Джихад» (Египетский исламский джихад)» «Братья-мусульмане» («Аль-Ихван аль-Муслимун», Египет, международная ТО); «Народный фронт освобождения Палестины»; «Конграгел» (бывшая Рабочая партия Курдистана); «Реальная ИРА» (Северная Ирландия) и ряд других. Деятельность большинства из них объявлена преступной и запрещена в большинстве стран.

Активное использование Интернета террористическими и экстремистскими организациями началось с 2000 г. и год от года развивается в геометрической прогрессии. Число сайтов, посвященных пропаганде расизма и насилия, по оценкам британского издания Guardian (со ссылкой на данные исследовательской организации Surf Control), только с января 2000 г. по апрель 2004 г. выросло на 26%. По сведениям Surf Control, масштабы роста числа расистских сайтов за первые 4 месяца 2004 г. сопоставимы с темпами увеличения их численности на протяжении всего 2003 г. Повышенная активность отмечается на сайтах различных религиозных группировок и арабских военизированных организаций, которые все чаще стали осваивать просторы сети. По мнению специалистов, на протяжении последних четырех лет число экстремистских сайтов выросло почти на 300%. При этом, если в 2000 г. было зарегистрировано 2 756 такого рода ресурсов, то в апреле 2004 г. их число уже перевалило за 10 000. Подобная негативная тенденция продолжает сохраняться и в настоящее время, и она полностью корреспондируется с распространением экстремизма и терроризма в Российской Федерации. Примечательно, что 55% сайтов, противоречащих британским законам, зарегистрированы в США, в их числе 23% экстремистских и порнографических сайтов с элементами насилия, которые инициированы из России [4, 7–14].

В настоящее время в сети Интернет имеется более ста активно действующих сайтов различных антироссийских радикальных структур. Они, как правило, содержат пропаганду антигосударственных и антиобщественных идей, а также проводят агитационную и вербовочную деятельность, направленную на увеличение числа сторонников экстремизма и терроризма. Особая опасность заключается в том, что данная тенденция активно набирает силу в российском обществе на фоне уже имеющихся в нем многочисленных правовых, кадровых, управленческих и иных проблем [3, 12, 15].

Проведенные авторами исследования показали, что начиная с 2012 г. количество объектов экстремистской и террористической направленности в России, использующих в своих преступных целях Интернет, увеличивается, причем эта тенденция наблюдается как в целом по России, так и в отдельных регионах. Например, в Дальневосточном федеральном округе (ДФО) данная проблема всерьез заявила о себе в 2004–2006 гг., когда глобальная сеть стала доступной практически по всей стране. С этого времени органами внутренних дел ДФО фиксируется деятельность радикальных групп по формированию в сетях негативного образа представителей государственной власти, распространению материалов, направленных на разжигание межнациональной и межконфессиональной вражды. Общедоступность распространяемой информации и ее быстрое тиражирование, как отмечают в ОВД ДФО, способствовали резкому увеличению в регионе числа сторонников радикальных объединений. В результате в 2008 г. в регионе был отмечен значительный рост количества выявленных экстремистских проявлений, сохраняемый и по настоящее время. Приведенные данные корреспондируются с информацией из других источников [4, 9, 13].

Не секрет, что неформальные радикальные движения, используя глобальную сеть, манипулируют общественным сознанием, создают себе образы борцов за права и свободы, подменяют факты и интерпретируют обстоятельства в свою пользу, чем привлекают на свою сторону отдельных лиц из числа молодежи, скрывая при этом противоправность своих намерений. Пропагандируемая такими движениями идеология подменяет позитивные морально-этические нормы общества, формирует у некоторой

(к счастью, небольшой) части общества асоциальное мировоззрение и поведение, на некоторое время делая из них своих сторонников. В результате правоохранительная и правоприменительная деятельность государственных органов воспринимается такими представителями общества как ущемляющая права человека [3, 4, 10, 11, 15].

Современные технологии Интернета позволяют преступникам не только активно осуществлять разовые экстремистские и террористические акции, но и эффективно решать вопросы, связанные с обеспечением более широкой реализации своих возможностей террористическими организациями, разработкой новых форм и методов информационно-психологического воздействия на людей, проведением их апробации. Одним из проявлений такой деятельности с использованием возможностей террористических организаций является разработка специальных информационно-коммуникационных технологий (ИКТ) по подготовке и осуществлению так называемых «оранжевых революций», их апробация и активное использование. Опасность таких ИКТ для государства и общества состоит в том, что действия экстремистской и/или террористической организации в ходе подобных революций активно маскируются под ***легальные демократические процессы***. Причем на определенном этапе использования данного вида технологий нередко может иметь место их ***комбинирование***. Подобным образом действовала, например, в 2011 г. организация «Братья мусульмане» в Египте[1] [3].

Экстремистские и террористические организации посредством интернет-ресурсов: получают и распространяют информацию; организуют проведение публичных мероприятий; организуют сбор пожертвований; взламывают банковские счета; ведут информационно-пропагандистскую и образовательную деятельность и привлекают к ней различного рода волонтеров; вербуют новых членов своих организаций; планируют и координируют совместные действия смежных экстремистских и террористических группировок [4, 5, 16]. Наиболее часто в экстремистской и террористической деятельности информационные сети используются для хакерских атак на системы управления важными объектами социальной инфраструктуры (транспорт, энергоснабжение и т.д.). Кибертеррористы могут также получать информацию об объектах, избранных ими для диверсий (например, о транспортной инфраструктуре, общественных зданиях, портах и т.п.), а также о планируемых контртеррористических мероприятиях [3, 11, 13, 16].

Особую тревогу вызывает использование механизмов кибертерроризма фактически на государственном уровне. В этой связи интересна ситуация, сложившаяся в Китае. Известно, что КНР не участвует в международном сотрудничестве по борьбе с киберпреступностью, не делится информацией, связанной с документированием имеющихся в данной сфере противоправных деяний. Однако при этом Китай осуществляет активную государственную поддержку разработки и совершенствования программ, связанных с незаконным получением информации через Интернет. Особую остроту проблема кибербезопасности приобрела после того, как на внутренние сети нескольких крупных IT-корпораций (среди которых были Apple и Microsoft) и СМИ были совершены хакерские атаки, предположительно, из китайского сегмента глобальной сети[2].

Сложившаяся ситуация привела к тому, что отдельные государства (в частности, Германия) вынуждены негласно сотрудничать с хакерами (естественно, не являющимися действующими сотрудниками государственных, военных и правоохранительных структур) и поднимать вопрос о создании специальной государственной структуры, обладающей указанными возможностями. Так, федеральная разведывательная служба Германии уже формирует специальное подразделение, призванное обеспечить кибербезопасность государственных ведомств и промышленных предприятий, о чем глава разведки ФРГ Г. Шиндлер проинформировал депутатов парламента. Количественный состав такого подразделения рассчитан на 130 специалистов, призванных оказать противодействие международным хакерам. Основная угроза для кибербезопасности Германии, по мнению Шиндлера, исходит из Китая, где хищением информации о высоких технологиях, принадлежащих другим странам, занимаются около 6 тыс. сотрудников военного ведомства. По его словам, на сотрудничество с хакерами, не находящимися на службе у государства, у разведывательного ведомства уходит слишком много средств. В дальнейшем создаваемой службой планируется набор кандидатов для работы среди студентов и выпускников немецких университетов.

[1] *Дичев Т., Бийчанинова А., Берестенко М.* Информационный Чернобыль // Советская Россия. 10.06.1993. № 68; *Соловьев А.И.* Принятие государственных решений: учеб. пособие. М.: КноРус, 2006. 344 с.

[2] URL: http://huyandex.com/blog/1162/37.html.

В России положение дел с противодействием интернет-преступности следующее. По сообщениям СМИ, к концу 2014 г. на государственном уровне должно было быть разработано так называемое киберкомандование, которое предполагалось сделать отдельным управлением в структуре Минобороны России либо наделить статусом командования рода войск[3]. Пока данная информация остается неподтвержденной, что вызывает у авторов озабоченность, поскольку нынешние действия международных террористических и экстремистских организаций на территории Российской Федерации по масштабам опасности можно сравнить с военными операциями. Более того, международный опыт показывает, что интернет-пространство в скором будущем может стать основной площадкой военных и террористических действий. Речь идет о возможном развязывании кибервойн с возможными убийствами реальных людей [7, 11, 16]. Головной центр НАТО по коллективной кибероборонe представил первое формализованное описание правил кибервойны, в котором собраны ссылки на международное законодательство, применимое к военным действиям в киберпространстве. Основная работа по подготовке этого свода правил проходила в Таллине, поэтому данный «научный труд» получил название «Таллинские инструкции». Самым примечательным в этом документе является указание на возможность физического уничтожения гражданских лиц, если будет доказано их участие во враждебных действиях против пострадавшей стороны[4].

Одними из ключевых участников кибервойн являются террористические и экстремистские организации. Как показывает современная международная практика, именно ими осуществляется инициация конфликтных ситуаций, требующих применения вооруженных сил. На еще более опасный уровень выходит практика использования террористическими и экстремистскими организациями социальных сетей. Подобные ресурсы, предоставляющие возможность свободно размещать информацию, становятся одним из наиболее эффективных средств влияния на значительное число пользователей Интернета. Ярким примером этого является массовое использование деструктивными силами социальных сетей и сервисов в Египте во время так называемой «Арабской весны», а подтверждением – динамика количества входов в социальную сеть Twitter в Египте в период с января по март 2010 г.[5] [5, 7, 11, 16].

Другим примером эффективного использования ИКТ в экстремистских и террористических целях являются организация и проведение так называемой «жасминовой революции» в Тунисе в 2010–2011 гг. До этого, вслед за ЮАР, Тунис считался одной из самых благополучных стран Африки. За годы правления президента Бен Али ВВП страны утроился, количество бедных тунисцев уменьшилось на 10%, а показатели продолжительности жизни, детской смертности, уровня образования, пенсионного обеспечения и т.п. стали самыми лучшими в арабском мире. Широкое распространение в стране получила сеть Интернет.

Отличительной чертой тунисской революции стало то, что в ходе ее проведения широко использовались социальные сети Facebook и Twitter, участники которых распространяли призывы к протестам, что позволило называть происходящее «цифровой», или Twitter-революцией. Оценивая ее итоги, некоторые эксперты высказывают мнение, что такая форма борьбы окончательно подорвала способность государств контролировать информационные потоки внутри своих стран и между ними, и отныне социальные сети могут стать надежной площадкой для народных движений. Это свидетельствует о повышении риска проведения «оранжевых революций» в различных странах, что и подтверждается событиями последних лет, происходившими в различных странах мира. Так, характерной чертой практически всех имевших место в последние годы выступлений народных масс в странах Северной Африки и Ближнего Востока было активное использование протестующими глобальной сети Интернет, в частности различных социальных сетей. Эти инструменты в руках «революционеров» позволяли им мобилизовать протестные настроения, координировать действия выступающих, информировать мировое сообщество о происходящих событиях. В настоящее время возможность запуска механизма беспорядков с использованием социальных сетей террористическими и экстремистскими организациями представляет реальную угрозу и для Российской Федерации [6, 11].

Отработанный сценарий «оранжевых» и прочих цветных революций стал опасен для нашей страны

[3] URL: http://huyandex.com/blog/1162/37.html.
[4] URL: http://soft.mail.ru/pressrl_page.php?id=51117.
[5] *Цымбурский В.Л.* Сверхдлинные военные циклы и мировая политика. URL: http://intelros.org/books/rythm_ros_3.htm.

в последний год, когда по соседству с Россией весной 2014 г. он был повторно реализован на Украине. Кроме того, нельзя не учитывать мнения экспертов о возможности апробации механизма проведения подобных революций в других странах из ближнего окружения Российской Федерации. Подтверждением возможности такой ситуации является следующий факт. Сирийские хакеры взломали сайт полномочного представительства президента России по ДФО и разместили на нем «обращение к российскому народу». По сведениям приморских СМИ, ответственность за кибератаку взяли на себя представители интернет-сообщества Syrian Revolution Electronic Suite. Злоумышленники предложили россиянам отказаться от поддержки президента Сирии Б. Асада и прекратить поставки Дамаску тяжелого вооружения. При этом они принесли свои извинения «всем хорошим русским людям» за взлом портала. Интернет-атака была осуществлена в ночное время, и обращение хакеров было доступно пользователям в течение всего нескольких часов, после чего сторонняя информация со страницы была удалена, и специалисты возобновили работу сайта. Ранее, в марте 2013 г., уже сторонниками сирийского лидера был осуществлен взлом аккаунта агентства Agence France Press (AFP) в Twitter, где они потребовали объективного освещения ситуации в Сирии[6].

Известно, что в социальных сетях Facebook и Twitter активно функционируют страницы радикальной афганской организации «Талибан». Более того, с мая 2011 г. для записей в них помимо языка пушту используется еще и английский. Двуязычие уже позволило талибам привлечь на свою страницу в твиттере более 5,5 тыс. подписчиков. В Российской Федерации социальные сети также широко используются террористическими организациями в регионах, где имеют место «тлеющие» этнические конфликты, прежде всего в Республике Дагестан. Российскими правоохранительными органами периодически фиксируются факты появления новых интернет-ресурсов, пропагандирующих радикальные религиозные течения, в целях вовлечения новых последователей. Так, 4 мая 2012 г. в Республике Дагестан была прекращена деятельность двух сайтов, признанных экстремистскими. Эти интернет-сайты, представленные как «официальные ресурсы», действовали в интересах бандподполья республики. На данных информационных ресурсах был выявлен факт размещения материалов радикальных исламистов Амира Сейфуллаха «Джихад против вероотступников» и Мухаммада ибн Сулеймана ат-Тамими «Китаб бат-Таухид» (Книга единобожия).

К апрелю 2013 г. на оперативном контроле правоохранительных органов находилось более 300 сайтов, блогов, микроблогов и других социальных сервисов сети Интернет, а также электронных СМИ. Среди них наиболее посещаемыми являются социальные сети «Одноклассники», «ВКонтакте», Facebook, «Живой Журнал» и Twitter, где нередко представители бандподполья ведут агитацию и пропаганду своих экстремистских идей. Ими обеспечено легендированное присутствие на этих ресурсах, что позволяет своевременно получать информацию о планах активистов несистемной оппозиции, подготавливаемых последними массовых акциях, в том числе несанкционированных.

В рамках выполнения Плана работы координационного Совета МВД РФ по информационному противоборству за 2012 г. из сети Интернет удалено 13 256 аудио- и видеоматериалов, внесенных в Федеральный список экстремистских материалов Министерства юстиции Российской Федерации. Прекращена деятельность 5 сайтов, в результате чего доступ к их материалам с признаками экстремизма был заблокирован для 930 тыс. пользователей, заблокировано 12 групп социальной сети «ВКонтакте».

В то же время следует отметить наличие ряда проблем, осложняющих построение эффективной системы выявления и раскрытия рассматриваемого вида противоправной деятельности террористических и экстремистских организаций. К наиболее серьезной из них следует отнести отсутствие в МВД РФ самостоятельного структурного подразделения, четко ориентированного на противодействие противоправной деятельности террористов и экстремистов по данному направлению. Организация такой структуры даст возможность решать кадровые проблемы по набору в подразделения МВД РФ профессиональных специалистов в этой области. Ввиду отсутствия в России нормативно-правовых актов, регламентирующих меры противодействия террористическим и экстремистским организациям, ГИАЦ МВД России не ведет прямого учета преступлений, совершаемых с использованием ресурсов Интернета. В то же время проблемы, очерченные в настоящей статье, требуют незамедлительного решения.

[6] URL: http://huyandex.com/blog/1155/80.html.

Список литературы

1. *Глезер В.Д.* Зрение и мышление. Ленинград: Наука, 1985. 248 с.
2. *Дятлов С.А.* Принципы информационного общества // Информационное общество. 2000. № 2. С. 77–85.
3. *Поздняков А.И.* Информационная безопасность личности, общества, государства // Военная мысль. 1993. № 10. С. 16.
4. *Пугачев В.П.* Информационно-финансовый тоталитаризм: российский эксперимент по американскому сценарию // Вестник Московского университета. Сер. Политические науки. 1999. № 4. С. 25.
5. *Райхель Ю.* Информационное оружие XXI века // Журналист. 2000. № 7. С. 9.
6. *Самсонов А., Авченко В.* Общество информационного контроля. URL: http://liv.piramidin.com/politica/samsonov_oik/samsonov_oik.htm.
7. *Андреев В.Г.* Оружие и война: новые тенденции развития // Военная мысль. 1999. № 3. С. 50.
8. *Антонян Ю.М., Кудрявцев В.Н., Эминов В.Е.* Личность преступника. СПб.: Юридический центр Пресс, 2004. 366 с.
9. *Виноградов М.В.* Терроризм: психологический портрет // Терроризм. Правовые аспекты борьбы: нормативные и международные правовые акты с комментариями. М.: ЭКСМО, 2005. 503 с.
10. *Ольшанский Д.В.* Психология терроризма. СПб.: Питер, 2002. 215 с.
11. *Иногамова-Хегай Л.В.* Проблемы международного терроризма в международном и российском уголовном праве. URL: http://kalinovsky-k.narod.ru/b/ufa20034/16.htm.
12. *Санаев А.* Русский PR в бизнесе и политике. М.: Ось-89, 2003. 144 с.
13. *Томас Т.Л.* Сдерживание асимметричных террористических угроз, стоящих перед обществом в информационную эпоху // Мировое сообщество против глобализации преступности и терроризма. М.: Международные отношения, 2002. 196 с.
14. *Тропина Т.Л.* Киберпреступность и кибертерроризм: поговорим о понятийном аппарате // Інформаціні технолог та безпека: Міжнародна науково-практична конференція. Вып. 3. Киев: Изд-во НАН Украины, 2003. С. 173–181.
15. *Богомолова Н.Н.* Социальная психология печати, радио и телевидения. М.: МГУ, 1991. 125 с.
16. *Попов М.О., Лукъянец А.Г.* Обеспечение военной безопасности в контексте информационной войны // Наука і оборона. 1999. № 2. С. 39–40.

ISSN 2311-875X (Online)
ISSN 2073-2872 (Print)

Threats and Security

NATIONAL INTERESTS: ACTUAL ISSUES OF COUNTERING TERRORIST AND EXTREMIST ORGANIZATIONS' USE OF THE INTERNET

Andrei A. MAIDYKOV[a,*], Oleg B. ISAROV[b]

[a] Research Institute of Ministry of Internal Affairs of Russian Federation, Moscow, Russian Federation
maydikov@mail.ru

[b] Research Institute of Ministry of Internal Affairs of Russian Federation, Moscow, Russian Federation
07070@lenta.ru

[*] Corresponding author

Article history:
Received 28 April 2015
Accepted 20 May 2015

JEL classification: P37

Keywords: Internet sources, social network, information networks, terrorism, extremism

Abstract

Importance The research reviews how terrorist and extremist organizations (TEO) use the Internet for their purposes. We overview the main areas for mitigating instances of extremism and terrorism in social networks.

Objectives We try to find solutions to some important tasks of legal and organizational nature, which, if resolved, will help to more effectively prevent TEO from using the Internet for their purposes.

Methods As part of the proposed methodological approach, we determine the key area for countering TEO's use of the Internet, in accordance with the existing priorities of the State policy.

Results We determine a structure and sequence of activities for identifying how TEO mainly use the Internet, the status and functional capabilities of those who intend terrorist and extremist activities via the World Wide Web. The article describes the current situation, proposes methods for effective and timely detecting, clearing and preventing terrorism and extremism. We also provide guidelines for solving security issues in countering TEO's use of the Internet.

Conclusions and Relevance The State should apply the proposed method for performance-based analysis of TEO's use of the Internet as a tool to effectively and precisely prevent and clear such crimes. The method is needed to control and manage Russia's plans and programs for national security, constructing and developing special law protection organizations, implementing new methods and legal mechanisms. The outcome of the research will facilitate the State planning, determining the sequence of and methods for performing objectives and tasks of developing the national strategy for law protection.

References

1. Glezer V.D. *Zrenie i myshlenie* [Vision and thinking]. Leningrad, Nauka Publ., 1985, 248 p.
2. Dyatlov S.A. Printsipy informatsionnogo obshchestva [Principles of information society]. *Informatsionnoe obshchestvo = Information Society*, 2000, no. 2, pp. 77–85.
3. Pozdnyakov A.I. Informatsionnaya bezopasnost' lichnosti, obshchestva, gosudarstva [Information security of individuals, society, State]. *Voennaya mysl' = Military Thought*, 1993, no. 10, p. 16.
4. Pugachev V.P. Informatsionno-finansovyi totalitarizm: rossiiskii eksperiment po amerikanskomu stsenariyu [Information and financial totalitarianism: the Russian experiment following the American scenario]. *Vestnik Moskovskogo universiteta. Ser. Politicheskie nauki = Bulletin of Moscow State University. Ser. Political Sciences*, 1999, no. 4, p. 25.
5. Raikhel' Yu. Informatsionnoe oruzhie XXI veka [Information weapons of the 21st century]. *Zhurnalist = Journalist*, 2000, no. 7, p. 9.
6. Samsonov A., Avchenko V. *Obshchestvo informatsionnogo kontrolya* [The society of information control]. Available at: http://liv.piramidin.com/politica/samsonov_oik/samsonov_oik.htm. (In Russ.)
7. Andreev V.G. Oruzhie i voina: novye tendentsii razvitiya [Weapons and war: new development trends]. *Voennaya mysl' = Military Thought*, 1999, no. 3, p. 50.

8. Antonyan Yu.M., Kudryavtsev V.N., Eminov V.E. *Lichnost' prestupnika* [Identity of the criminal]. St. Petersburg, Yuridicheskii tsentr Press Publ., 2004, 366 p.

9. Vinogradov M.V. *Terrorizm: psikhologicheskii portret. V kn.: Terrorizm. Pravovye aspekty bor'by: normativnye i mezhdunarodnye pravovye akty s kommentariyami* [Terrorism: a psychological portrait. In: Terrorism. Legal aspects of the struggle: regulatory and international legal acts with commentary]. Moscow, EKSMO Publ., 2005, 503 p.

10. Ol'shanskii D.V. *Psikhologiya terrorizma* [Psychology of terrorism]. St. Petersburg, Piter Publ., 2002, 215 p.

11. Inogamova-Khegai L.V. *Problemy mezhdunarodnogo terrorizma v mezhdunarodnom i rossiiskom ugolovnom prave* [Issues of global terrorism in the international and Russian criminal laws]. Available at: http://kalinovsky-k.narod.ru/b/ufa20034/16.htm. (In Russ.)

12. Sanaev A. *Russkii PR v biznese i politike* [The Russian PR in business and politics]. Moscow, Os'-89 Publ., 2003, 144 p.

13. Thomas T.L. [Deterring asymmetric threats to the society in the era of information]. *Mirovoe soobshchestvo protiv globalizatsii prestupnosti i terrorisma: materially mezhdunarodnoi konferetsii* [Proc. Int. Sci. Conf. Global Community against Globalization of Crime and Terrorism]. Moscow, Mezhdunarodnye otnosheniya Publ., 2002, 196 p.

14. Tropina T.L. [Cybercrime and cyberterrorism]. Інформаціні технолог та безпека: Міжнародна науково-практична конференція. Kiev, NAS of Ukraine Publ., 2003, pp. 173–181.

15. Bogomolova N.N. *Sotsial'naya psikhologiya pechati, radio i televideniya* [Social psychology of the press, radio and television]. Moscow, MSU Publ., 1991, 125 p.

16. Popov M.O., Luk'yanets A.G. Obespechenie voennoi bezopasnosti v kontekste informatsionnoi voiny [Ensuring the military security in the context of information warfare]. *Наука і оборона*, 1999, no. 2, pp. 39–40.