Министерство образования и науки
Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего профессионального образования
«ЮЖНЫЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Материалы лекций (опорных тезисов) для работы индивидуальных пропагандистов

Ростов-на-Дону 2010

Содержание

1. Лекция «Международное сотрудничество как основа для антитеррористической деятельности»

Целевая группа: руководители среднего и низшего звена региональных органов власти, органов местного самоуправления и аппарата АТК

План:

1. Терроризм: истоки, виды, стратегии борьбы.

2. Нормативно-правовая база Российской Федерации в сфере противодействия терроризму.

3. Международное сотрудничество – краткая характеристика международных организаций.

4. Международный банк данных.

5. Дальнейшие перспективы.

Вопросы для дискуссионного обсуждения

Список использованной литературы

Рекомендуемая литература по проблеме

Печатные издания

Электронные издания

Приложение (Словарь терминов)

1. Терроризм: истоки, виды, стратегии борьбы

В начале третьего тысячелетия мировое сообщество лицом к лицу столкнулось с террористической угрозой. И, хотя терроризм не является новообразованием конца XIX – XXI веков, его истоки можно проследить еще в древнем мире (иудейская секта сикариев) и в средние века (секта Хашашаинов). В настоящее время он стал всеохватывающим явлением. Можно сказать, что современный мир шагнул не только в эпоху глобализации, но и в эпоху тотального противодействия терроризму.

Однако на сегодняшний день не существует общепринятого юридического определения терроризма. В Кодексе законов США, титул 22 раздел 2656 ф(д) он квалифицируется как «предумышленное, политически мотивированное насилие, совершаемое против мирного населения или объектов субнациональными группами или подпольно действующими агентами, обычно с целью повлиять на настроение общества». В российском праве терроризм определяется как «идеология насилия и практика воздействия на общественное сознание, на принятие решений органами государственной власти, органами местного самоуправления или международными организациями, связанные с устрашением населения и/или иными формами противоправных насильственных действий» [11, ст.3 п. 1].

Существует несколько **классификаций видов терроризма** в зависимости от выделяемого критерия.

Так, по ***характеру субъекта террористической деятельности*** терроризм делится на [8]:

– неорганизованный, или индивидуальный (терроризм одиночек) – в этом случае теракт (реже, ряд терактов) совершает один-два человека, за которыми не стоит какая-либо организация (Дмитрий Каракозов, Вера Засулич, Равашоль и др.);

– организованный, коллективный – террористическая деятельность планируется и реализуется некой организацией (народовольцы эсеры, Аль-Каида, ИРА, ЭТА, государственный терроризм). Данный вид терроризма является наиболее распространенным в современном мире.

По ***адресату террористического акта*** говорят о [8]:

– терроризме оппозиционеров по отношению к власти и терроризме самих властей, государственном терроризме, терроризме как направлении государственной политики;

– терроризме индивидуальном, при котором адресатами терактов являются конкретные лица в силу их личных действий или принадлежности к

определенной группе или организации (русские цари и государственные сановники; Анвар Садат, Индира Ганди) и терроризме массовом, или слепом, в отношении случайных людей (взрывы в Оклахоме, Москве, Волгодонске);

– уголовном терроризме.

В зависимости от ***целей*** выделяют следующие виды терроризма [8]:

– националистический – преследует сепаратистские или национально-освободительные цели;

– религиозный – может быть связан с борьбой приверженцев религии между собой (индуисты и мусульмане, мусульмане и христиане) и внутри одной веры (католики-протестанты, сунниты-шииты), и преследует цель подорвать светскую власть и утвердить власть религиозную (Исламистский терроризм);

– идеологически заданный, социальный – преследует цель коренного или частичного изменения экономической или политической системы страны, привлечения внимания общества к какой-либо острой проблеме (анархистский, эсеровский, фашистский, европейский «левый», экологический терроризм и др.). Этот вид терроризма также называют революционным.

Современный международный терроризм имеет разнообразные формы: это необъявленные войны и экспорт революций и контрреволюций, массовые взрывы и политические убийства, захват самолетов и кораблей, государственных учреждений, посольств и общественных и образовательных учреждений, похищения, избиения и издевательства, ограбления банков, ювелирных магазинов и многое другое [3].

Среди наиболее часто используемых **стратегий борьбы с терроризмом** выделяют следующие [8]:

– стратегия, допускающая частичные уступки требованиям террористов – выплату выкупа, территориальные и моральные уступки

(например, признание лидеров террористов равноправными партнерами по переговорам и т.д.);

– стратегия, нацеленная на безоговорочное уничтожение террористов и их сторонников, а также поощрение лиц, идущих на сотрудничество с «демократическими» государствами в их борьбе с террором, отказ от каких бы то ни было переговоров с террористами, отказ от заключения перемирий.

2. Нормативно-правовая база Российской Федерации в сфере противодействия терроризму

Правительство Российской Федерации выработало ряд нормативно-правовых актов, определяющих политику нашего государства в сфере противодействия терроризму.

К основным документам относятся:

– Уголовный кодекс РФ от 13 июня 1996 г. № 63-ФЗ. Глава 24. Преступления против общественной безопасности. Статья 205 [9];

– Указ Президента РФ от 15 февраля 2006 г. № 116 «О мерах по противодействию терроризму» (с изменениями от 02.08.2006) [10];

– Положение о Национальном антитеррористическом комитете (утвержденное Указом Президента РФ от 15 февраля 2006 г. № 116) (с изменениями от 02.08.2006) [4];

– Федеральный закон Российской Федерации от 6 марта 2006 г. № 35-ФЗ «О противодействии терроризму» [11];

– Положение об Антитеррористической комиссии в субъекте Российской Федерации (утвержденное Национальным антитеррористическим комитетом 7 июля 2006 г.) [5];

– Концепция противодействия терроризму в Российской Федерации [2].

В частности, в Разделе 2 пункт 5 Концепции противодействия терроризму в Российской Федерации говорится: «Общегосударственная

система противодействия терроризму представляет собой совокупность субъектов противодействия терроризму и нормативных правовых актов, регулирующих их деятельность по выявлению, предупреждению (профилактике), пресечению, раскрытию и расследованию террористической деятельности, минимизации и (или) ликвидации последствий проявлений терроризма».

В Разделе 2 пункт 12 указывается, что «Противодействие терроризму в Российской Федерации осуществляется по следующим направлениям:

а) предупреждение (профилактика) терроризма;

б) борьба с терроризмом;

в) минимизация и (или) ликвидация последствий проявлений терроризма» [2].

В Российской Федерации создается система противодействия терроризму [6], на федеральном уровне она представлена Национальным антитеррористическим комитетом [7].

3. Международное сотрудничество – краткая характеристика международных организаций

В современных условиях глобализации мировых процессов практика показывает, что разрозненные действия отдельных стран не достаточны для эффективного противостояния терроризму. Сегодня терроризм не является проблемой отдельно взятого региона или страны, а превратился в одну из наиболее острых проблем, существенно подрывающую внутриполитическое и социально-экономическое развитие ряда государств мира, реально угрожающую их национальной безопасности. Осознание опасности распространения международного терроризма и возможности перенесения порожденных им вооруженных конфликтов на территории других государств поставило мировое сообщество перед необходимостью создания международной системы борьбы с данным видом преступной деятельности. Оценивая состояние и угрозу расширения терроризма на ближайшее

будущее, мировое сообщество едино во мнении, что эффективность борьбы с этим явлением зависит не только от мер, которые принимаются на уровне национальных спецслужб, правоохранительных органов, других учреждений и организаций, на которые возложены задачи борьбы с терроризмом, но и от координации политики и сотрудничества государств на многосторонней основе, в том числе в рамках международных организаций, институтов и форумов, вырабатывающих общие подходы к этой проблеме.

В большинстве стран созданы собственные **специальные контртеррористические структуры** [1], представленные в Таблице 1:

Таблица 1. Контртеррористические структуры зарубежных стран

Страна	**Структура**	**Адрес**	**Цели и задачи**
Австрийская Республика	Федеральное ведомство по защите конституции и борьбы с терроризмом (BVT)	http://www.bmi.gv.at/	Борьба с деятельностью иностранных разведок, террористическими проявлениями, экстремизмом, организованной преступностью, незаконной миграцией.
	Группа антитеррора «Cobra»		– борьба с терроризмом и организованной преступностью; – освобождение заложников, аресты, связанные с большим риском, борьба с похищениями людей; – защита и охрана важных персон; – антитеррористическое сопровождение полетов; – участие в программе защиты свидетелей; – обеспечение охраны австрийских представительств за

Страна	Структура	Адрес	Цели и задачи
			границей.
Республика Беларусь	Антитеррористический центр (АТЦ) КГБ		– организацию и координацию деятельности подразделений органов государственной безопасности в целях достижения согласованности их действий по предупреждению, выявлению и пресечению террористических акций, вскрытию и устранению причин и условий, способствующих их подготовке и реализации; – обеспечение взаимодействия с субъектами, непосредственно осуществляющими борьбу с терроризмом, а также с другими государственными органами, участвующими в предупреждении, выявлении и пресечении террористической деятельности в пределах своей компетенции; – обеспечение деятельности оперативного штаба по управлению контртеррористической операцией, участие в ведении переговоров с террористами; – установление и поддержание рабочих контактов с АТЦ СНГ, международными центрами и организациями, занимающимися вопросами борьбы с терроризмом.
Соединенное Королев	Единое полицейское подразделение по	www.security.homeoffice.gov.uk/,	Основной замысел – объединить ресурсы всех служб и подразделений

Страна	Структура	Адрес	Цели и задачи
ство Великобритании и Северной Ирландии	борьбе с терроризмом (S015)	www.mi5.gov.uk/output/terrorism.html	полиции, задействованных в борьбе с терроризмом. Работает в тесном контакте с контрразведкой МИ-5, разведывательными структурами, а также Королевской прокурорской службой.
	Контртеррористический научно-технический центр (КНТЦ)		КНТЦ предназначен для технического обеспечения действий вооруженных формирований Министерства обороны и других ведомств по борьбе с терроризмом, и ликвидации последствий терактов.
	Комиссия по вопросам безопасности и терроризма (КВБТ)		Решение вопросов общей стратегии по борьбе с терроризмом.
	Группа квалифицированных сотрудников Единого антитеррористического подразделения		Организация антитеррористической работы с позиций территориальных органов Скотланд-Ярда, дислоцированных в 32 районах Большого Лондона.
Грузия	Антитеррористический центр МВД	www.police.ge/index.php	– добывание информации относительно возможных террористических актов против президента Грузии, других высокопоставленных лиц и членов их семей, физических или юридических лиц находящихся под защитой государства или международной защитой; – вскрытие подготовки и предотвращение террористических актов

Страна	Структура	Адрес	Цели и задачи
			политического характера; – вскрытие подготовки и предотвращение террористических актов направленных против государственных, стратегических, политических или экономических интересов Грузии; – вскрытие активности террористических организаций и незаконных вооруженных формирований, действующих на территории Грузии и пресечение их действий; – противодействие международному терроризму и незаконной миграции; – проверка возможных контактов и оказание помощи иностранным гражданам принудительно вовлеченным в антигосударственную деятельность и находящихся на территории Грузии в составе террористических организаций; – вскрытие и предотвращение фактов незаконного приобретения ядерного, радиоактивного, химического, бактериологического или любого другого вещества, представляющего опасность человеческой жизни и здоровью, а так же их незаконного присвоения с террористической целью.

Страна	Структура	Адрес	Цели и задачи
Королевство Дания	Антитеррористический центр (АТЦ)	http://www.pet.dk/English.aspx	Обобщение информации, имеющей отношение к безопасности страны с точки зрения террористической угрозы.
Государство Израиль	Контртеррористический комитет при Совете национальной безопасности Израиля	www.terrorism-info.org.il/site/home/default.asp	Анализ и обобщение информации о внутренних и внешних угрозах государству.
Королевство Испании	Национальный координационный антитеррористический центр (НКАЦ)	http://www.guardiacivil.org/index.jsp, http://www.mir.es/	Информационно-аналитическое подразделение, призванное в режиме реального времени отслеживать ситуацию в области борьбы с терроризмом, проводить анализ складывающейся обстановки, выявлять и прогнозировать террористические угрозы, своевременно предупреждать о них правительство страны, предоставлять ему предполагаемые сценарии развития событий и давать соответствующие рекомендации для принятия решений.
Республика Казахстан	Центр антитеррористических программ (ЦАП)	http://www.knb.kz	Содействие информационной, научной, организационной и материально-технической поддержке всех субъектов, участвующих в программах и проектах по борьбе с терроризмом и экстремизмом.
Китайская Народная Республ	Министерство общественной безопасности	http://www.gov.cn	Выполняет задачи по борьбе с организованной преступностью, коррупцией, терроризмом, осуществляет охрану общественного

Страна	Структура	Адрес	Цели и задачи
ика			порядка, контролирует каналы въезда-выезда из страны.
Республика Молдова	Антитеррористический Центр (АТЦ) Службы информации и безопасности (СИБ)	http://www.sis.md	– техническое координирование мер по предупреждению и борьбе с терроризмом; – анализ, хода проведения антитеррористических мероприятий органами власти; – оценка факторов риска и террористических угроз национальной безопасности; – разработка и введение в действие национальной системы оповещения в случае террористической угрозы; – создание и администрирование специализированного банка данных, организаций и лиц, относящихся к международному терроризму, их финансового обеспечения.
Республика Монголия	Координационный совет (КС) по борьбе с терроризмом Главного разведывательного управления (ГРУ)	http://pmis.gov.mn/	Координационная деятельность – на регулярной основе проводятся консультативные встречи, в ходе которых уточняются позиции по интересующим вопросам, вырабатываются направления взаимодействия в борьбе с терроризмом и экстремизмом.
Палестинская Национальная Админи	Служба общей безопасности	http://www.gcc.gov.ps	Проведение операций против повстанцев и террористов, выявление лиц, сотрудничающих с Израилем.

Страна	Структура	Адрес	Цели и задачи
страция			
Португальская Республика	Разведывательная служба безопасности (РСБ)	http://www.sis.pt	Борьба против террористической угрозы и связанных с ней организованной преступности, нелегальной миграции, незаконного оборота наркотиков и оружия, распространения элементов оружия массового поражения (ОМП), а также националистических движений.
Румыния	Антитеррористический оперативный координационный центр (АОКЦ)	www.mai.gov.ro	– осуществляет координацию специальных мероприятий, путем задействования представителей от учреждений и общественных институтов, входящих в Национальную Систему Противодействия и Борьбы с Терроризмом (НСПБТ); – обеспечивает оперативный обмен данными и информацией между министерствами и ведомствами, входящими в НСПБТ, по вопросам деятельности, связанной с противодействием террористический угрозе; – осуществляет анализ полученных данных в целях своевременного принятия необходимых мер; – организует отслеживание террористической активности и оперативное информирование государственных учреждений и общественных организаций,

Страна	Структура	Адрес	Цели и задачи
			задействованных в НСПБТ.
	Антитеррористическая группа «Acvila» («Орел»)		Выявление и отслеживание фактов использования систем телекоммуникаций и средств связи в интересах обеспечения деятельности террористических организаций и организованных преступных группировок, а также недопущение использования финансовых институтов страны для «отмывания» денежных средств.
Соединенные Штаты Америки	Национальный Контртеррористический центр (НКЦ)	http://www.nctc.gov/about_us/about_nctc.html	– координация разведывательной аналитики 16 американских спецслужб; – обеспечение стратегического планирования и поддержки операций, направленных на предотвращение терактов.
Украина	Антитеррористический Центр (АТЦ) при Службе Безопасности Украины (СБУ)	http://www.sbu.gov.ua/sbu/control/uk/	Межведомственная координация деятельности органов исполнительной власти всех уровней, направленная на предупреждение и силовое пресечение террористических актов в отношении государственных деятелей, критических объектов жизнеобеспечения населения, объектов повышенной опасности, актов, угрожающих жизни и здоровью большого количества людей.
Французская Республика	Центр по координации борьбы с терроризмом (UCLAT)	http://www.interieur.gouv.fr/	Координирующий орган

Страна	Структура	Адрес	Цели и задачи
	Национальное управление по борьбе с терроризмом (DNAT)		Задачи идентификации, выявления местонахождения и захвата лиц, совершивших теракты, и их сообщников.
	Отделение борьбы с финансированием терроризма		Право «замораживания» используемых террористами банковских счетов вне зависимости от легальности источников поступления денежных средств.
	Служба оперативной документации		Выявление каналов финансирования террористической деятельности.
	Управление общего осведомления (RG)		Контроль деятельности политических партий и общественных организаций, иностранцев (исключая подозреваемых в шпионаже), средств массовой информации, разработка террористических групп, контрразведывательное обеспечение среднего и малого бизнеса.
Федеративная Республика Германия	Антитеррористический ситуационный центр	http://www.bmi.bund.de/	Анализ сведений, связанных с террористическими угрозами, оперативный обмен информацией между национальными спецслужбами.
Чешская Республика	Информационная служба безопасности (ИСБ)	http://www.bis.cz/, http://www.mvcr.cz/	Разработка и планирование контртеррористических мероприятий, организация обмена информацией с зарубежными партнерами в США и ЕС.
Япония	Следственное управление общественной безопасности	http://www.moj.go.jp/	Борьба с терроризмом, наркобизнесом и организованной преступностью.

Кроме того, для борьбы с международной преступностью и терроризмом созданы специальные Межгосударственные структуры (Таблица 2.).

Таблица 2. Контртеррористические межгосударственные структуры

Структура	**Адрес**	**Цели и задачи**
Антитеррористический центр государств-участников Содружества Независимых Государств (АТЦ СНГ)	http://www.cis.minsk.by/main.aspx?uid=6668	Обеспечение координации взаимодействия компетентных органов государств-участников СНГ в борьбе с международным терроризмом и иными проявлениями экстремизма.
Международная организация уголовной полиции – Интерпол	http://www.interpol.ru/	Способствует международному полицейскому сотрудничеству, поддерживает и помогает всем организациям, властям и службам, миссия которых состоит в том, чтобы предотвратить или противостоять международным преступлением.
Контртеррористический комитет Совета Безопасности Организации Объединенных Наций	http://www.un.org/russian/sc/ctc/	Содействует укреплению потенциала государств – членов Организации Объединенных Наций по предотвращению террористических актов как на национальном, так и межрегиональном уровне.

4.Международный банк данных

В 2007 г. в средствах массовой информации было объявлено о создании при активном участии Национального антитеррористического комитета Международного банка данных по противодействию терроризму в целях укрепления международного сотрудничества. Основная цель данного банка данных заключается в формировании единой межгосударственной

информационной системы обеспечения антитеррористической деятельности. В банке данных созданы самостоятельные разделы, в которых накапливается информация о средствах идеологического воздействия террористов, а также об инструментах для осуществления контрпропаганды. Доступ к банку данных могут иметь только спецслужбы и правоохранительные органы любого государства, заключившего соответствующее соглашение с Национальным антитеррористическим комитетом. Однако Национальный антитеррористический комитет считает, что наряду с бизнес-структурами академические и коммерческие научные сообщества призваны сыграть ключевую роль как в разработке и внедрении новых технологий для усиления мер охраны и безопасности, так и в проведении исследований по вопросам, связанным с терроризмом, включая изучение структурных и других факторов, которые могут способствовать радикализации и вербовке террористов.

Сегмент открытой информации международного банка данных по противодействию терроризму может быть плодотворно использован для совместной работы силовых структур и представителей различных научных, образовательных и общественных организаций над:

– созданием системы противодействия идеологии терроризма (Раздел 2 пункт 13 а);

– противодействием распространению идеологии терроризма путем обеспечения защиты единого информационного пространства Российской Федерации; совершенствование системы информационного противодействия терроризму (Раздел 2 пункт 15 б);

– разработкой мер и осуществлением профилактических мероприятий по противодействию терроризму на территориях субъектов Российской Федерации (Раздел 2 пункт 15 е);

– обеспечением скоординированной работы органов государственной власти с общественными и религиозными организациями

(объединениями), другими институтами гражданского общества и гражданами» (Раздел 2 пункт 15 л Концепции противодействия терроризму в Российской Федерации [2]).

5. Дальнейшие перспективы

В заключении необходимо еще раз отметить, что терроризм сегодня носит транснациональный характер, и решать данную проблему возможно только совместными усилиями всех членов мирового сообщества, что приводит к необходимости разработки комплексных международных подходов и единых методов противостояния различным террористическим проявлениям. При этом первостепенную роль в предотвращении террористических актов имеют не только скоординированные совместные действия всех участников мирового сообщества, но и своевременное получение информации. Эффективное решение этой проблемы возможно при активном взаимодействии различных стран и использования сегмента открытой информации международного банка данных по противодействию терроризму.

Целесообразно было бы также создание в рамках международного банка данных по противодействию терроризму отдельного раздела, к которому бы имели доступ различные общественные, научные и образовательные организации. Цель выделения такого раздела – создание единого гражданского информационного пространства: взаимообмен контактами, опытом и информацией о проводимых мероприятиях, расширение сотрудничества с различными международными гражданскими антитеррористическими организациями.

Кроме того, перспективой антитеррористической деятельности также является не только совершенствование механизмов дальнейшего развития международного сотрудничества, но, в особенности, пропаганда идеологии гражданского общества и формирование гуманитарных ценностей, которые

будут способствовать формированию позитивного общественного сознания, исключающего саму возможность использования насилия для достижения каких-либо целей.

Вопросы для дискуссионного обсуждения

1. Особенности терроризма XXI века и его исторические, социальные и другие предпосылки.

2. Современный терроризм – это «проблема» отдельно взятой страны или всего мирового сообщества?

3. Современные стратегии противодействия терроризму. Политика двойных стандартов отдельных государств.

4. Особенности нормативно-правовой базы Российской Федерации. Структуры и возможности для противодействия.

5. Иностранные и международные организации, участвующие в антитеррористической деятельности.

6. Международный банк данных по противодействию терроризму:

1) Какая информация должна находиться в разделе открытого доступа (в общем пользовании), а какая должна быть «ДСП» (для служебного пользования)?

2) Как должен быть организован доступ к сегменту открытой информации международного банка данных по противодействию терроризму?

3) При каких условиях организациям и другим лицам должен предоставляться доступ к банку? Критерии отбора организаций и частных лиц?

4) Необходимо ли популяризировать информацию о банке данных в СМИ и в Интернет-ресурсах и почему?

5) Что может являться источником для пополнения банка данных? Какая информация и каким образом должна попадать в международный банк данных?

7. Перспективы международного сотрудничества для формирования установок антитеррористического мышления.

Список использованной литературы

1. Зарубежные контртеррористические структуры – http://nak.fsb.ru/nac/cooperation.htm

2. Концепция противодействия терроризму в Российской Федерации –

3. Королев А.А. Международный терроризм на современном этапе – Электронный журнал «Знание. Понимание. Умение». 2008, № 6. –

4. Положение о Национальном антитеррористическом комитете (утвержденное Указом Президента РФ от 15 февраля 2006 г. № 116) (с изменениями от 2 августа 2006 г.) –

5. Положение об Антитеррористической комиссии в субъекте Российской Федерации (утвержденное Национальным антитеррористическим комитетом 7 июля 2006 г.)

6. Система противодействия терроризму в Российской Федерации – http://nak.fsb.ru/nac/structure.htm

7. Структура аппарата Национального антитеррористического комитета – http://nak.fsb.ru/nac/institution/structure.htm

8. Уголовный кодекс РФ от 13 июня 1996 г. № 63-ФЗ. –

9. Указ Президента РФ от 15 февраля 2006 г. № 116 «О мерах по противодействию терроризму» (с изменениями от 2 августа 2006 г.) –

10. Федеральный закон Российской Федерации от 6 марта 2006 г. № 35-ФЗ –

Рекомендуемая литература по проблеме:

Печатные издания

1. Беликов С.В. Молодежные БТО и ксенофобия в России. // Свободная мысль. 2007, № 12.

2. Васильев Н. Неизбежность диалога. // Литературная газета. 2007, № 46.

3. Галахов С.С., Тарсуков К.М. Терроризм – угроза государственности России в XXI в. (исторические, правовые, праксеологические проблемы). // Правовая наука на рубеже XXI столетия: Сб. науч. трудов. – Омск, 2000.

4. Гевелинг Л.В. Коррупционные формы политического финансирования: материальная основа распространения терроризма. // Финансовый мониторинг потоков капитала с целью предупреждения финансового терроризма. – М.: Изд-во МНЭПУ, 2005.

5. Горшков А.Ф. Глобальная война с международным терроризмом. // Независимое военное обозрение. 2005, № 1.

6. Гришко А.Я. Личность террориста: Криминологический портрет. – Рязань, 2006.

7. Добрынина В., Кухтевич Т. Экстремизм как проявление девиантности и деликвентности. // Наука, культура, общество. 2006, № 7.

8. Дугин А. Геополитика постмодерна. – М., 2005.

9. Жаринов К.В. Терроризм и террористы: Ист. справочник. – Мн.: Харвест, 1999. – 606 с.

10. Золотарев П.С. Международный терроризм – истоки возникновения и перспективы развития. // Социальные и математические средства измерения потенциала общественной безопасности в субъектах Российской Федерации. – М., 2006.

11. Иванов О.В. Информационная составляющая современных войн. // Вестник Московского университета. Сер. 18. Социология и политология. 2004, № 4.

12. Ильинский И.М. О терроре и терроризме. // Между будущим и прошлым. – М., 2006.

13. Ильясов Ф.Н. Архетипы поло-репродуктивного поведения и конфликт западноевропейской и исламской цивилизаций. // Человек, 2005. № 2.

14. Ильясов Ф.Н. Терроризм – от социальных оснований до поведения жертв. // Социологические исследования. 2007, № 6.

15. Королев А.А.Террор и терроризм в психологическом и идеологическом измерении: история и современность. – М.: Московский гуманитарный университет, 2008.

16. Нетаньяху Беньямин. Война с терроризмом: Как демократии могут нанести поражение сети международного терроризма. Пер. с англ. – М.: Альпина Паблишер. 2002. – 207 с.

17. Путилин Б.Г. Террористический интернационал. – М.: Кучково поле, 2005. – 320 с.

18. Рубан Л.С. Дилемма XXIго века: толерантность и конфликт. – М., 2006.

19. Руло Эрик. Добро, зло и «терроризм». // La Monde diplomatigue. 2007, Май.

20. Сборник документов Совета Европы в области защиты прав человека и борьбы с преступностью. – М.: “Спарк”, 1998.

21. Хоффман Брюс. Терроризм – взгляд изнутри. Пер. с англ. – М.: Ультра Культура, 2003. – 264 с.

22. Яновский К., Жаворонков С., Затковецкий И. и др. Политико-экономические аспекты борьбы с терроризмом – М.: ИЭПП, 2005 (Научные труды № 82).

Электронные издания

1. Адвокат террора. Главные герои. – http://www.arthouse.ru/attachment.asp?id=8006

2. Будницкий О.В. Терроризм: история и современность – http://www.irex.ru/press/pub/polemika/10/bud/

3. Влияние информационного обеспечения антитеррористических операций – http://antiterror.ru/library/lections/70865105

4. Журавель В.П. «Об актуальном в противодействии идеологии терроризма» – Журнал «Право и безопасность» № 2 (27), Июль 2008 – http://www.dpr.ru/pravo/pravo_23_20.htm

5. Ильин Е.П. «Актуальные проблемы противодействия вовлечению молодежи в террористическую деятельность» – http://nak.fsb.ru/nac/media/publications/article.htm!id%3D10288046@cmsArticle.html

6. Ильин Е.П. «О современной ситуации в сфере противодействия терроризму в России» – http://nak.fsb.ru/nac/structure.htm

7. Ильясов Ф.Н. Терроризм – от социальных оснований до поведения жертв. Социологические исследования, 2007, № 6 – http://www.iliassovfn.narod.ru/article/terror/terrorizm.htm

8. Кагарлицкий Б. Анатомия террора. // Журнал «Свободная мысль», 2005, № 4. – http://www.scepsis.ru/library/id_194.html

9. Координация борьбы с международным терроризмом http://www.atcsng.ru/articles.cgi?id=78

10. Координация контртеррористических мероприятий, осуществляемых в рамках и вне системы ООН – http://www.un.org/russian/terrorism/cttaskforce.shtml

11. Особенности состояния, поведения и деятельности людей в экстремальных ситуациях с витальной угрозой – http://antiterror.ru/library/lections/70865178

12. Панарин И.Н. Антитеррористическая стратегия России. Информационное противодействие террору – http://www.km.ru/magazin/view.asp?id=68740D2EC6C04AB68439DAA2D5058DC0

13. Противодействие использованию террористическими и экстремистскими организациями возможностей сети Интернет – http://www.atcsng.ru/articles.cgi?id=322

14. Социально-культурные предпосылки терроризма – http://antiterror.ru/library/lections/70864959

15. Тарасов А. «Терроризм становится кислородом политики» в книге: «Сто дней одного века». – М.: АНО РИА «Общая газета», 2000. – http://saint-juste.narod.ru/terror.htm

16. Террористическая ментальность: контрмеры – http://web.archive.org/web/20080119102933/http://usinfo.state.gov/journals/itps/0507/ijpr/ijpr0507.htm

17. Угрозы из киберпространства – http://www.atcsng.ru/pressrelations.cgi?id=205

18. Храмчихин А. Бой с тенью. Теория терроризма. – http://www.chaskor.ru/p.php?id=1212

19. Экстремизм в глобальной паутине – http://antiterror.ru/library/151536639

Приложение

Словарь терминов

Агрессия – поведение, ориентированное на нанесение вреда объектам, в качестве которых могут выступать живые существа или неодушевленные предметы. Агрессивное поведение служит формой реагирования на физический и психический дискомфорт, стрессы, фрустрации. Кроме того, оно может выступать в качестве средства достижения какой-либо значимой цели, в том числе повышения собственного статуса за счет самоутверждения.

Выученная беспомощность – психологическое состояние, включающее нарушения в мотивации, когнитивных и эмоциональных процессах, возникающее вследствие пережитой субъектом неподконтрольности.

Ксенофобия – нетерпимость к кому-либо или чему-либо чужому, незнакомому, непривычному. Восприятие чужого как непонятного, непостижимого, а поэтому опасного и враждебного. Воздвигнутое в ранг мировоззрения, может стать причиной вражды по принципу национального, религиозного или социального деления. Также иногда может трактоваться буквально, как навязчивый страх перед другими людьми, то есть фобия в клиническом смысле.

Культура межнационального общения – совокупность специальных знаний и убеждений, соответствующих им поступков и действий, совершаемых в межличностных контактах и при взаимодействии представителей различных этнических групп, позволяющих быстро и качественно достигать взаимопонимания и согласия.

Личностные ценности – «консервированные» отношения с миром, обобщенные и переработанные совокупным опытом социальной группы. Они ассимилируются в структуру личности и в дальнейшем своем функционировании практически не зависят от ситуативных факторов.

Национализм – идеология и направление политики, базовый принцип – ценность нации как высшей формы общественного единства и ее первичности в государствообразующем процессе. Он опирается на национальное чувство, родственное патриотизму. Отличается многообразием течений, некоторые из них противоречат друг другу. Проявления крайнего национализма, включая разжигание межнациональной розни и этническую дискриминацию, относятся к международным правонарушениям.

Ненависть – стойкое активное отрицательное чувство человека, направленное на явления, противоречащие его потребностям, убеждениям, ценностям. Ненависть способна вызвать не только соответствующую оценку предмета, но и агрессивное поведение, направленное против него. Ненависть самоподдерживается и разжигается, легко выходя за пределы разумного.

Нетерпимость – нежелание или невозможность терпеть кого-либо или что-либо.

Предубеждение – установка, препятствующая адекватному восприятию сообщения или действия. Как правило, предубеждение не осознается и рассматривается человеком как следствие объективной самостоятельной оценки каких-либо фактов.

Радикализм– крайняя, бескомпромиссная приверженность каким-либо взглядам, концепциям; стремление доводить политическое или иное мнение до его конечных логических и практических выводов, не принимая ни каких компромиссов.

Расизм – идеи об изначальном разделении людей на высшие и низшие расы, из которых первые являются создателями цивилизации и призваны господствовать над вторыми. Осуществление расистских теорий на практике порой находит свое выражение в политике расовой дискриминации.

Расовая дискриминация – любое различие, исключение, ограничение или предпочтение, основанное на признаках расы, цвета кожи, родового, национального или этнического происхождения, имеющие целью или

следствием уничтожение или умаление признания, использования или осуществления на равных началах прав человека и основных свобод в политической, экономической, социальной, культурной или любых других областях общественной жизни.

Страх – эмоция, возникающая в ситуациях угрозы биологическому или социальному существованию индивида и направленная на источник действительной или воображаемой опасности. В отличие от боли и других видов страдания, вызываемых реальным действием опасных для существования индивида факторов, страх возникает при их предвосхищении. В зависимости от характера угрозы интенсивность и специфика переживания страха варьируются в широком диапазоне оттенков: опасения, боязнь, испуг, ужас.

Террор – политика устрашения, подавления политических противников насильственными методами.

Терроризм – крайняя форма проявления экстремизма – использование насилия или угрозы его применения в отношении отдельных лиц, группы лиц или различных объектов с целью достижения политических, экономических, идеологических и иных выгодных террористам результатов. Основная цель – вызвать состояние ужаса не только у своих жертв-заложников, но и у всех остальных людей. Появление и распространение терроризма обусловлено комплексом причин, среди которых выделяют: глобализационные, социально-политические, правовые, экономические, идеологические, организационно-управленческие, психологические.

Толерантность – стремление и способность к установлению и поддержанию общности с людьми, которые отличаются в некотором отношении от превалирующего типа или не придерживаются общепринятых мнений.

Установка – готовность, предрасположенность субъекта, возникающая при предвосхищении им появления определенного объекта и

обеспечивающая устойчивый целенаправленный характер протекания деятельности по отношению к данному объекту. Психофизиологические и психологические механизмы, реализующие различные операциональные установки, проявляются в общем тонусе организма, выражающем позу субъекта в целом, определенную преднастройку сенсорной и моторной области, что предшествует развертыванию тех или иных способов осуществления действия.

Фанатизм – твердая и не признающая никаких аргументов безальтернативная приверженность личности каким-либо идеям, верованиям, или представлениям, обычно сочетающаяся с нетерпимостью к чужим взглядам и убеждениям, исключающая критическое восприятие чего-либо и определяющая практически любую активность личности и ее оценочное отношение к окружающему миру. Виды фанатизма: религиозный; политический, идеологический; этнический, национальный, расовый, а также фанатизм среди спортивных болельщиков и т.п.

Шовинизм – агрессивная идеология и политика – крайний национализм, проповедующий национальную и расовую исключительность и превосходство и разжигающий национальную вражду и ненависть.

Экстремизм – приверженность к крайним взглядам и радикальным мерам, крайнее проявление чего-либо: действий, высказываний, взглядов и т.п. Может быть политическим, религиозным, экономическим, социальным и т.д. Политический экстремизм – осуществление политики крайними методами.

2. Лекция «Позитивная и негативная роль СМИ в формировании образа террориста у молодого поколения»

Целевая группа: руководящие работники (среднее и низшее звено) региональных и муниципальных департаментов и министерств образования, учителя, педагоги, в том числе институтов повышении квалификации в системе образования, журналисты, студенты факультетов журналистики и филологии

План:

1) Основные понятия психологии терроризма.

2) Признаки терроризма.

3) Психологическая характеристика террористов и мотивов их преступного поведения.

4) СМИ как эффективное средство формирования общественного мнения.

5) Проблема ответственности представителей СМИ за освещение событий.

6) Групповая дискуссия по вопросу: «Что же можно и нужно предпринять сегодня для того, чтобы предотвратить ситуации, в которых СМИ вольно или невольно становятся «подельниками» террористов?».

7) Рекомендации журналистам.

Как явление терроризм имеет социальную природу и политическую направленность. Он порожден социальными противоречиями, при их обострении проявляет тенденцию к усилению и направлен на достижение противоправным и общественно опасным способом политических целей в интересах определенных государств, социальных сил, организаций и движений.

Будучи сложным, многоплановым явлением, отражая интересы различных политических сил, терроризм подчас характеризуется в науке, политике весьма неоднозначно и противоречиво.

Этимологически термин «терроризм» происходит от латинского слова «террор», которое означает страх, ужас, вызванный жестокими насильственными действиями властей или отдельных лиц. В социально-психологическом аспекте терроризм нередко понимается как использование террора в тех или иных целях, для обеспечения интересов различных социальных групп.

В мировой науке существуют два основных подхода к понятию «терроризм». Биологических подход связывает это явление с некоей «насильственной сущностью человека», «естественным» стремлением людей угрожать интересам других и использовать любые средства для достижения своих целей. Социально-психологический подход, хотя и характеризуется большим разнообразием оценок роли и механизм влияния тех или иных социальных факторов, обусловливающих терроризм, признает определяющее значение социальной среды, социальных процессов в его возникновении.

В качестве достаточно распространенных определений терроризма можно привести следующие. По мнению американских исследователей В. Маллисона и С. Маллисона, террор «есть систематическое использование крайнего насилия и угрозы насилием для достижения публичных или политических целей». Более развернутое определение дается в докладе межведомственной комиссии по борьбе с терроризмом, созданной в США в 1985 году Дж. Бушем, бывшим тогда вице-президентом: «терроризм – это противоправное использование или угроза использования насилия против лиц или объектов для достижения политических или социальных целей. Обычно он направлен на запугивание или принуждение правительств, групп или отдельных лиц для изменения политики или действий». Некоторые исследователи характеризуют терроризм как «войну XX века». В более широком плане определяют терроризм известные юристы-международники Н.Б. Крылов и Ю.А. Решетов: «под терроризмом в самом широком значении этого термина понимают акты насилия или угрозу насилием, цель которых –

внушить страх и заставить действовать или воздержаться от действий в нужном террористам направлении». Связывая терроризм чаще всего с политическими и идеологическими целями тех сил, которые его используют, специалисты выделяют достаточно широкий спектр социальных противоречий и иных явлений, обуславливающих его. К ним относят социально-экономические и политические противоречия, национальные, религиозные, идеологические конфликты.

Изучая терроризм как социально-психологическое явление, входящее в систему политического экстремизма, следует обратить внимание на важнейшие признаки терроризма.

Итак, к основным признакам (особенностям) терроризма, отражающим сущность его как социально-психологического и политического явления, относятся:

- применение насилия и устрашения, которое достигается использованием особо острых форм и методов;

- направленность на достижение политических целей, на ослабление политических противников;

- повышенная общественная опасность, связанная с непосредственной угрозой жизни людей, нелегитимность;

- использование конспирации как необходимого условия существования террористических структур и результативности их действий;

- опосредованный способ достижения политического результата – через совершение посягательств на жизнь и здоровье людей (независимо от их причастности или непричастности к противникам террористов).

С учетом сказанного можно определить терроризм следующим образом. Терроризм – это система использования насилия для достижения политических целей посредством принуждения государственных органов, международных и национальных организаций, государственных и общественных деятелей, отдельных граждан или их групп к совершению или

отказу от совершения тех или иных действий в пользу террористов путем нелегитимного применения силы или угрозы ее применения к конкретным лицам или к любым другим лицам и группам.

На современном этапе развития общества профессиональных террористов и террористические организации можно отнести к некой субкультурной группе лиц, которые взяли на вооружение идеи террора, имеют специфические представления о социальной справедливости, своеобразную, зачастую искаженную картину обустройства мира.

По признанию самих террористов, «терроризм – это оружие слабых», то есть оружие тех лиц, которые не могут достичь своих целей законным путем. Члены террористических организаций и групп весьма неоднородны по своему составу, идеологической ориентации, уровню образования, мотивам, которыми они руководствуются при совершении террористических акций. Сравнительные исследования психологии терроризма показывают, что не существует никакого единого «террористического» сознания. Говорить о преобладающем типе террориста весьма трудно, так как среди них есть «идеалисты», «нигилисты», «мстители», хладнокровные рационалисты и импульсивно действующие убийцы.

К личностным качествам преступников, осуществляющих террористические акты, относятся жестокость, авантюризм, демонстративность, стремление любыми методами заявить о себе, добиться хотя бы кратковременной власти над другими людьми. Одна из психологических черт террориста это тенденция к экстернализации (поиску или переносу во вне источников личных проблем). Другие характерные черты – постоянная оборонительная готовность, чрезмерная поглощенность и незначительное внимание к чувствам других (черствость). Исследования социального окружения террористов показали, что 25 % их членов потеряли одного или обоих родителей в возрасте до 14 лет, треть привлекалась к

уголовной ответственности, прослеживается значительное число неудач в образовании, профессиональной деятельности и личной жизни.

Для молодых людей, которые составляют подавляющее большинство членов террористических групп, террористическая деятельность может стать привлекательной, благодаря возможности самоутвердиться, ощутить собственную значимость, преодолеть отчуждение и фрустрацию. Кроме того, к мотивам участия в террористической деятельности относятся:

Во-первых, примитивное, черно-белое мировосприятие, практически никогда не анализирующее конечные цели и результаты террора.

Во-вторых, ощущение своего превосходства над «простыми смертными», что отменяет или уменьшает разборчивость в средствах террора. В-третьих, малая чувствительность в отношении своих и чужих страданий при высокой готовности убивать и умирать. Для террористов, жизнь которых отличалась социальной изоляцией и личными неудачами, террористическая организация становится семьей, которой у них никогда не было. Таким образом, внутренний, личный кризис превращается в разделенный с другими, тоже пострадавшими от общества индивидами, в ненависть, направленную во вне. Для индивидов, угнетенных комплексом неполноценности, страдающих о т дефицита самоуважения и с недостаточно развитой социализированной личностью, слияние с группой имеет фундаментальное значение: группа становится для них главной и единственной системой нормальных стандартов и ценностей. Поэтому одна из общих черт террористов – потребность в принадлежности к группе.

Значительное место в деятельности террористов занимают и корыстные, материальные интересы, которые могут прикрываться политическими целями.

Учет психологических характеристик террористов и мотивов их преступного поведения способствует не только более успешному планированию и проведению антиррористических операций, но и позволяет

осуществлять общепредупредительную, профилактическую деятельность, особенно необходимую в молодежной среде. В настоящее время в системе подразделений безопасности разных стран не существует единой информационной базы, в которой бы содержались систематизированные биографические и психологические данные о террористах и сведения об их деятельности. Создание такой базы могло бы помочь накоплению информации на основе, которой можно вести предупредительно – профилактическую работу и создавать обобщенный портрет лиц, участвующих в террористических акциях или склонных к их совершению.

Способность СМИ быть эффективным средством формирования общественного климата давно подмечена, оценена и максимально используется людьми, пытающимися решать проблемы достижения своих политических, экономических, национальных, религиозных, социальных и иных целей опосредованным путем влияния на группы и слои граждан. Причем полярность этого влияния в зависимости от стоящих задач может быть и положительной и отрицательной.

Ярким примером активного использования уникальных возможностей СМИ для достижения собственных целей незаконными, преступными путями является обращение к ним экстремистов и террористов. Заметим, что акции терроризма, как правило, предполагают либо рефлексивное реагирование на них СМИ, либо прямое обращение к ним с требованием довести до общественности цели и требования субъектов террористической деятельности. И в том, и в другом случае предполагается, что через возможности телевидения, радио, печатных изданий террористы смогут обратиться к представителям органов власти и широкой общественности для разъяснения своих задач, пропаганды идеологии, а в некоторых случаях – и для получения поддержки своим нелегитимным, преступным действиям со стороны отдельных социальных групп и слоев населения.

На фоне разрастающейся угрозы терроризма в глобальном масштабе опросы об ответственности представителей СМИ за освещение событий, связанных с террористическими акциями, не раз становились предметом заинтересованной дискуссии специалистов и общественности.

Репортер Ассоциации общественных информационных станций в Бонне Эберхард Плис предостерегал коллег от опасности «быть использованными» террористами в преступных целях. О необходимости повышения журналистской этики в деле освещения проблем терроризма говорил и редактор «Армейского радио» в Израиле Нахман Шелл, приводивший примеры безнравственного смакования некоторыми американскими корреспондентами деталей человеческих трагедий. Созвучно с этими предостережениями и мнение российского военного аналитика Владимира Васильева, считающего, что «сообщение об инциденте должно быть кратким и сухим. Незачем смаковать жуткие подробности. О реальных трагических последствиях произошедшего достаточно знать соответствующим органам, близким и родственникам. Не более того». Помощник генерального директора Британской информационной компании в Лондоне Алан Протхироу, признавая высокий технологический уровень американской журналистики, также отмечал нарушения с их стороны норм этики и стандартов хорошего вкуса в профессиональной деятельности

Весьма актуальным в современных условиях является вопрос о правомерности и целесообразности предоставления теле- и радиоэфира террористам. Президент Эн-Би-Си Ларри Гроссман как-то признал: «Телевидение стало обыкновенным средством общения террористов с людьми». А редактор «Нью репаблик» Чарльз Кротхаммер добавляет: «Так как террористы не могут купить телевизионного времени, они вынуждены «зарабатывать» его террористическими акциями».

Освещение средствами массовой информации террористических акций зачастую сопряжено и с другими негативными, а порой и необратимыми

драматическими последствиями, даже если речь при этом не идет о пропаганде целей и идей терроризма. Особенно актуально это обстоятельство для актов терроризма, сопряженных с захватом заложников.

Так, во время захвата в 1977 г. лайнера западногерманской авиакомпании «Люфтганза», следовавшего в Магадишо, находившиеся на борту террористы из радиорепортажа узнали, что экипаж передает информацию об обстановке в самолете наземным службам. После этого один из пилотов, Юрген Буман, был расстрелян террористами. Боевикам движения «Тупака Амару», захватившим в декабре 1996 г. заложников резиденции японского посла в столице Перу Лиме, также именно из сообщений корреспондентов СМИ стали известны и факт нахождения среди удерживаемых лиц брата президента страны, что создавало реальную опасность для его жизни, и план подготовки контртеррористическими подразделениями специального подземного туннеля под здание резиденции посла.

СМИ способны не только затруднять проведение специальных контртеррористических операций или содействовать пропаганде идей терроризма, но и служить источником информации о тактике подготовки преступных действий и наиболее эффективных формах и методах реализации террористических намерений.

Далее аудитории предлагается вступить в дискуссию по вопросу:

Что же можно и нужно предпринять сегодня для того, чтобы предотвратить ситуации, в которых СМИ вольно или невольно становятся «подельниками» террористов?

Широкое распространение, в первую очередь, среди сотрудников спецслужб и правоохранительных органов, получило мнение о необходимости законодательного ограничения прав журналистов на получение и распространение информации, связанной с освещением террористической и антитеррористической деятельности, а также

ужесточения их ответственности в случаях нарушения установленных рамок. Во многих западных странах приняты законы и иные нормативные акты, достаточно жестко регулирующие порядок освещения событий в нестандартных, кризисных, чрезвычайных ситуациях. Так, например, министерством обороны США 14 января 1991 г. были приняты «Основные правила и руководство для СМИ», где журналистам запрещалось разглашение информации, способной поставить под угрозу жизнь людей.

Правильнее всего было бы говорить о грамотном регулировании порядка и процесса информирования общественности, как о проявлениях терроризма, так и об анти- и контртеррористической деятельности в нашей стране.

Определенные шаги в этом направлении уже предприняты. Так, статья 4 Закона Российской Федерации «О средствах массовой информации» запрещает использование СМИ для призыва к захвату власти, насильственному изменению конституционного строя и целостности государства, разжигания национальной, классовой, социальной, религиозной нетерпимости или розни, для пропаганды войны. Определенные ограничения для журналистов вводит и статья 15 «Информирование общественности о террористической акции» упоминавшегося уже Федерального закона «О борьбе с терроризмом». В этой статье говорится, что «информирование общественности о террористической акции и ее освещение средствами массовой информации осуществляется в формах и объеме, определяемых руководителем оперативного штаба по управлению контртеррористической операцией или представителем указанного штаба, ответственным за поддержание связи с общественностью». При этом «не допускается распространение информации: 1) раскрывающей специальные технические приемы и тактику проведения контртеррористической операции; 2) способной затруднить проведение контртеррористической операции и создать угрозу жизни и здоровью людей, оказавшихся в зоне проведения

операции или находящихся за пределами указанной зоны; 3) служащей пропаганде или оправданию терроризма и экстремизма; 4) о сотрудниках специальных подразделений, членах оперативного штаба по управлению контртеррористической операцией при ее проведении, а также о лицах, оказывающих содействие в проведении указанной операции».

Дискуссия.

1. Могу ли я критически оценивать ситуацию и, самое главное, объективно просчитывать последствия своих репортажей с места событий?

Мнение ведущего: информацию нужно так дозировать и облекать в такие формы, чтобы она не нанесла моральных травм родным и близким заложников, не поставила бы под угрозу жизнь и здоровье последних.

2. Как расценивается передаваемая мною информация рядовым обывателем? Не выгляжу ли я лицом, разделяющим платформу террористов или оправдывающим их насильственные действия?

Мнение ведущего: через корреспонденции красной нитью должна проходить идея о недопустимости применения насилия, какими бы лозунгами оно не оправдывалось. Насилие может породить только насилие Оно антигуманно, противоправно, наказуемо.

3. В каком объеме следует давать «живой эфир»? Стоит ли демонстрировать террористов, интервьюировать их, если оказался на месте драматических событий?

Мнение ведущего: нужно отдавать себе отчет в том, что стремление прорваться к массовой аудитории – одна из задач террористов. Снимая их на видеокамеру или предоставляя микрофон, журналист в известном смысле превращается в соучастника преступления. Другое дело, если фиксация конкретных действий террориста (без передачи в эфир) может способствовать формированию вещественных доказательств для будущего следствия. Целесообразна также подготовка и трансляция материалов, формирующих и укрепляющих у общественности негативное отношение к

террористам (наглое, вызывающее поведение, употребление наркотиков, пьянство). Кроме того, кино- и видеосъемка террористов может использоваться и как средство их сдерживания от каких-то крайних, жестоких поступков по отношению к заложникам.

4. Можно ли предавать гласности сведения о находящихся в руках террористов заложниках?

Мнение ведущего: надо иметь в виду, что такого рода информация станет и достоянием террористов. Если в ней будут раскрыты ранее не известные им данные, способные ухудшить положение заложников и тем более создать угрозу для их жизни и здоровья (вспомним ситуацию с шестью американскими дипломатами), то это недопустимо. Если же в эфир можно выдать информацию, способную смягчить отношение террористов к заложникам (например, жертвы оказались единоверцами, соплеменниками, земляками террористов), такую возможность следует максимально использовать.

5. Можно ли обращаться для получения уточняющей информации к родственникам заложников?

Мнение ведущего: от таких действий нужно отказаться. Даже если журналист хочет просто выразить человеческое участие родственникам потерпевшего, любой звонок или посещение представителя СМИ будет оцениваться ими однозначно негативно, как попытка погреть руки на чужой беде. Не следует усугублять ситуацию, травмируя психику людей.

Работники СМИ обязаны понимать, что в период теракта и контртеррористической операции спасение людей и право человека на жизнь первичны по отношению к любым другим правам и свободам.

В случае получения информации о готовящемся теракте или о его начале до обнародования данной информации журналист обязан сообщить ее руководству своего СМИ.

Журналисты должны иметь при себе и по первому требованию предъявлять редакционное удостоверение или иной документ, удостоверяющий личность и профессиональную принадлежность.

Руководство СМИ обязано незамедлительно передавать в распоряжение Оперативного Штаба или официальных органов ставшую им известной информацию, которая могла бы быть использована для спасения жизни людей.

Исходя из того, что доступ к СМИ с целью изложения своей позиции в большинстве случаев является одной из главных целей террористов, СМИ не должны:

- брать у террористов интервью по своей инициативе во время теракта кроме как по просьбе или с санкции Оперативного Штаба;

- предоставлять террористам возможности выйти в прямой эфир без предварительных консультаций с Оперативным Штабом;

- самостоятельно брать на себя роль посредника (за исключением случаев, когда это санкционировано и сделано по просьбе Оперативного Штаба);

- если представитель СМИ оказался в числе переговорщиков, он должен воздерживаться от собственных публикаций до разрешения кризиса;

- брать в руки оружие и надевать камуфляжную или иную униформу; понимать, что, взяв в руки оружие, работник СМИ перестает быть таковым;

- предлагать террористам, заложникам, другим вовлеченным в конфликт лицам предпринимать какие-либо действия для получения удачных видео- или фотокадров;

- оскорблять и унижать террористов, в руках которых жизнь заложников.

СМИ должны:

- помнить, что прямой теле- и радиоэфир может использоваться террористами для передачи условных сигналов сообщникам в других местах;

- избегать детальных подробностей о действиях профессионалов, занятых спасением людей;

- быть тактичными и внимательными к чувствам родных и близких жертв терроризма; проявлять особую чуткость к очевидцам событий как к источникам информации;

- избегать излишнего натурализма при показе места события и его участников, с уважением относиться к нравственным, национальным и религиозным чувствам своей аудитории;

- быть внимательным к употреблению тех или иных терминов в освещении событий; нельзя идти на поводу у террористов, использующих выгодные для себя самоназвания;

- отдавать себе отчет в том, что заложники террористов являются и заложниками ситуации, в определенный момент превращающимися в инструмент давления на общественное мнение;

- избегать идентификации родственников и друзей заложников и потенциальных жертв без их согласия.

Освещая теракты и антитеррористические операции нужно также:

- помнить о своей обязанности информировать общественность, а не сеять панику; следить не только за смыслом сказанного, но и за тоном;

- помнить, что сообщение в СМИ являются общедоступными, в том числе и для тех, кто намеренно создает критическую ситуацию;

- учитывать, что мировое сообщество отвергает связь терроризма с какой – либо конкретной религией, расой или национальностью;

- понимать, что информационные сообщения не должны содержать сведений, которые могли бы способствовать усилению позиций террористов, например, выступления в поддержку их требований. Подобные жесткие требования могут распространяться исключительно на ситуации, связанные с непосредственной угрозой для жизни людей, и не могут распространяться на

события политической, экономической или социальной борьбы, укладывающейся в рамки Конституции.

СМИ могут сообщать своей аудитории, что часть информации закрыта Оперативным Штабом на время проведения контртеррористической операции по соображениям безопасности для сохранения жизни людей.

Рекомендуемая литература:

1. Противодействие использованию террористическими и экстремистскими организациями возможностей сети Интернет (http://www.atcsng.ru/articles.cgi?id=322) (выступление А.П. Новикова 15.09.2008);

2. Как противостоять информационному агрессору. Интервью И. Плугатарева, «Время Союза», № 44 (49) от 10 ноября 2008 года);

3. *Новикова Г.В.* Сильная стратегия слабых. Террор в конце XX века // Политические исследования. 2000. № 1. С. 169.

4. Глобальная контртеррористическая стратегия (см.: http://www.un.org/russian/terrorism/framework.shtml). 8 сентября 2006 г.

5. Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-коммуникационных сетей международного информационного обмена»,

6. Доктрина информационной безопасности Российской Федерации, утверждена Президентом Российской Федерации 09.09.2000 № Пр-1895 // Российская газета. № 187. 2000.

7. Воскобоев А.И. Технологии убеждающего воздействия: особенности применения в практике учебного процесса. Северо-Кавказский психологический вестник № 4, 2009 г. С. 67-72.

8. Каракозов Р.Р. Организация смыслопоисковой активности человека как условие осмысления жизненного опыта// Психология с

человеческим лицом: гуманистическая перспектива в постсоветской психологии/ под ред. Д.А. Леонтьева, В.Г. Щур. М.: Смысл, 1997. С. 257-273.

9. Василюк Ф.Е. Психология переживания. М.: М.: Изд-во Моск. ун-та, 1984, - 200 с.

10. Панасюк А.Ю. Психология риторики: теория и практика убеждающего воздействия / А.Ю. Панасюк.- Ростов н/Д.: Феникс, 2007. – 208 с. – (Современные психотехнологии).

11. Ожиганов Э.Н. Профиль терроризма: природа, цели и мотивация // Социологические исследования. 2006. № 2. С. 53. Джемаль Г.Д. Освобождение ислама. М., 2004. С. 139.

12. Mallison W.T., Mallison S.V. The concept of Public Purpose Terror in International Law // Journal of Palestine Studies. Winter 1975. V. 4. № 2. P. 36.

13. Ольшанский Д.В. Психология терроризма. СПб., 2002. С. 56.

14. Skubiszewski K. Definition of Terrorism // Israel Yearbook on Human Rights. 1989. Vol. 19. P. 39–53;

3. Лекция «Понятие информационной безопасности и основное содержание угроз информационной безопасности России»

Целевая группа: учителя, преподаватели высшей школы, журналисты, работники (среднее и низшее звено) региональных и муниципальных департаментов молодежной политики и министерств образования.

План:

1) Понятие информационной безопасности.

2) Внешние и внутренние угрозы информационной безопасности России.

Информация - это важнейшая составляющая жизнедеятельности современного общества. В официальных документах ЮНЕСКО информация определяется как универсальная субстанция, пронизывающая все сферы человеческой деятельности, служащая проводником знаний и мнений, инструментом общения, взаимопонимания и сотрудничества, утверждения стереотипов мышления и поведения. Современное российское общество также трудно представить без широкого применения информационных и телекоммуникационных технологий, являющихся одним из факторов социально-экономического развития нашей страны.

Благотворное воздействие на развитие демократических институтов и процедур оказывает расширение национального информационного пространства. За четыре года количество зарегистрированных в России печатных средств массовой информации выросло на 40%, электронных - почти в 2,5 раза. Постоянная российская аудитория Интернета увеличилась за это время более чем в 4 раза и превысила сегодня 25 млн. человек[1].

Законодательно информационная сфера (среда) определена как сфера деятельности субъектов, связанная с созданием, преобразованием и потреблением информации. В состав информационной сферы входят:

---

[1] Послание Президента Российской Федерации Федеральному Собранию Российской Федерации от 26 апреля 2007 г. о важнейших общенациональных задачах // http://www.mgkirov.ru/doc/2007/04/26/polnyj-tekst-poslaniya-prezidenta-federalnomu-sobraniyu-rossijskoj-federatsii-26-apre

- субъекты информационного взаимодействия или воздействия;

- собственно информация, предназначенная для использования субъектами информационной сферы;

- информационная инфраструктура, обеспечивающая возможность осуществления обмена информацией между субъектами;

- общественные отношения, складывающиеся в связи с формированием, передачей, распространением и хранением информации внутри общества.

Прежде чем раскрыть понятие информационной безопасности, необходимо дать более общее понятие - понятие безопасности. Закон РФ «О безопасности»[2] определяет безопасность как «состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз». К основным объектам безопасности относятся:

- личность - ее права и свободы;

- общество - его материальные и духовные ценности;

- государство - его конституционный строй, суверенитет и территориальная целостность.

В Концепции национальной безопасности Российской Федерации[3] сформулированы такие социально-правовые категории, как «национальная безопасность Российской Федерации» и «национальные интересы». Под национальной безопасностью понимается «безопасность ее многонационального народа как носителя суверенитета и единственного источника власти в Российской Федерации». Понятие национальных интересов России трактуется как совокупности сбалансированных интересов личности, общества и государства в экономической, внутриполитической,

---

[2] Ст. 1 Закона РФ «О безопасности» от 5 марта 1992 г. № 2446-1 (в последней ред. от 26.06.2008 № 103-ФЗ) // ВСНД и ВС РФ. 1992. № 15. Ст. 769.

[3] Указ Президента РФ «Об утверждении Концепции национальной безопасности Российской Федерации» от 17 декабря 1997 г. № 1300 (в ред. Указа Президента Российской Федерации от 10.01.2000 № 24) // Собрание законодательства РФ. 2000. № 2. Ст. 170.

социальной, международной, информационной, военной, пограничной, экологической и других сферах.

Национальные интересы России в информационной сфере заключаются в соблюдении конституционных прав и свобод граждан в области получения информации и пользования ею, в развитии современных телекоммуникационных технологий, в защите государственных информационных ресурсов от несанкционированного доступа.

В Концепции подчеркивается, что в последнее время усиливаются угрозы национальной безопасности Российской Федерации в информационной сфере. Серьезную опасность представляют собой следующие факторы: стремление ряда стран к доминированию в мировом информационном пространстве, вытеснению России с внешнего и внутреннего информационного рынка; разработка рядом государств концепции информационных войн, предусматривающей создание средств опасного воздействия на информационные сферы других стран мира; нарушение нормального функционирования информационных и телекоммуникационных систем, а также сохранности информационных ресурсов, получение несанкционированного доступа к ним.

Таким образом, национальная безопасность РФ существенным образом зависит от обеспечения информационной безопасности[4].

Для раскрытия сущности информационной безопасности принято рассматривать следующие два понятия:

- безопасность информации – безопасность содержательной части (смысла) информации, т.е. отсутствие в ней побуждения человека к негативным действиям, умышленно заложенных механизмов негативного воздействия на человеческую психику или негативного воздействия на иной блок информации (например, информация, содержащаяся в программе для ЭВМ, именуемой компьютерным вирусом);

[4] Раздел IV Концепции национальной безопасности Российской Федерации»

- защита информации - защищенность информации от внешних воздействий (попыток неправомерного копирования, распространения, модификации (изменения смысла) либо уничтожения)[5].

В законодательстве Российской Федерации отсутствует определение информационной безопасности. В то же время само понятие встречается в таких актах, как Закон Российской Федерации от 5 марта 1992 г. № 2446-1 «О безопасности», Федеральный закон от 3 апреля 1995 г. № 40-ФЗ «О Федеральной службе безопасности»[6], Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-коммуникационных сетей международного информационного обмена»[7], Указ Президента Российской Федерации от 12 июня 2006 г. № 601 «Вопросы межведомственных комиссий Совета Безопасности Российской Федерации»[8], и ряде других.

Единственным документом, определяющим понятие «информационная безопасность», является утвержденная Президентом Российской Федерации в 2000 г. Доктрина информационной безопасности Российской Федерации[9]. Информационная безопасность Российской Федерации, согласно п.1 указанного документа, - это состояние защищенности ее национальных

---

[5] Лапина М.А., Ревин А.Г., Лапин В.И. Информационное право: учебное пособие / Под ред. И.Ш. Килясханова. – М.: ЮНИТИ-ДАНА, Закон и право, 2004. – С. 211.

[6] Федеральный закон «О Федеральной службе безопасности» от 3 апреля 1995 № 40-ФЗ (в последней ред. ФЗ от 04.12.2007 № 328-ФЗ) // Собрание законодательства РФ. 1995. № 15. Ст. 1269.

[7] Указ Президента Российской Федерации «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-коммуникационных сетей международного информационного обмена» от 17 марта 2008 № 351 (в ред. Указа Президента РФ от 21.10.2008 № 1510) // Собрание законодательства РФ. 2008. № 12. Ст. 1110.

[8] Указ Президента Российской Федерации «Вопросы межведомственных комиссий Совета Безопасности Российской Федерации» от 12 июня 2006 г. № 601 (в ред. Указа Президента РФ от 01.11.2008 № 1575 // Собрание законодательства РФ. 2006. № 25. Ст. 2698.

[9] Доктрина информационной безопасности Российской Федерации, утверждена Президентом Российской Федерации 09.09.2000 № Пр-1895 // Российская газета. № 187. 2000.

интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства[10].

Вышеупомянутая Доктрина, представляющая собой лишь совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации и не носящая нормативного характера, является в настоящее время единственным документом, закрепляющим методы обеспечения информационной безопасности Российской Федерации, основные положения государственной политики обеспечения информационной безопасности Российской Федерации и первоочередные мероприятия по ее реализации; организационную основу системы обеспечения информационной безопасности Российской Федерации. В этой Доктрине получили развитие положения, ранее закрепленные в Концепции национальной безопасности Российской Федерации[11].

Интересы личности в информационной сфере заключаются, во-первых, в реализации конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а во-вторых, в защите информации, обеспечивающей личную безопасность.

Интересы общества в информационной сфере заключаются в обеспечении интересов личности в этой сфере, упрочении демократии, создании правового социального государства, достижении и поддержании общественного согласия, в духовном обновлении России.

Интересы государства в информационной сфере состоят в создании условий для гармоничного развития российской информационной инфраструктуры, для реализации конституционных прав и свобод человека и

---

[10] Гришина В.В. Правовое обеспечение информационной безопасности // Административное и муниципальное право. – 2008. – № 5. – С.27.

[11] Куняев Н.Н. Информационная безопасность как объект правового регулирования в Российской Федерации // Юридический мир. - 2008. - № 2. – С.4.

гражданина в области получения информации и пользования ею в целях обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности России, политической, экономической и социальной стабильности, в безусловном обеспечении законности и правопорядка, развитии равноправного и взаимовыгодного международного сотрудничества[12].

Подводя итог сказанному, можно заключить:

Возрастание роли информации, информационных ресурсов и технологии в XXI веке выводят вопросы информационной безопасности России на первый план в системе обеспечения национальной безопасности страны. Именно информация выступает основным связующим звеном всех компонентов государственной политики в единое целое. Укрепление информационной безопасности названо в Концепции национальной безопасности РФ в числе важнейших долгосрочных задач.

Обеспечение информационной безопасности - это не только защита информации, но и организационные, правовые и другие меры, направленные на обеспечение устойчивого, стабильног развития общества и государства; при которых достигаются следующие цели: конфиденциальность информации; целостность информации и связанных с ней процессов (создания, ввода, обработки и вывода); доступность информации; учет всех процессов, связанных с информацией.

Юридическая наука должна принимать участие в решении всех поставленных задач и реализации соответствующих целей обеспечения информационной безопасности. При этом ее приоритет должен обеспечиваться в двух областях:

- во-первых, в определении разумного баланса между правом субъектов на свободное получение информации путем ее сбора или доступа к имеющимся ресурсам и правом субъектов на установление ограничений в

[12] Лапина М.А., Ревин А.Г., Лапин В.И. Информационное право: учебное пособие / Под ред. И.Ш. Килясханова. – М.: ЮНИТИ-ДАНА, Закон и право, 2004. – С. 212.

указанных действиях со стороны, иных лиц по отношению к сведениям, обладателями которых они являются;

- во-вторых, в разработке и реализации правовых мер защиты информации, доступ к которой должен ограничиваться по правомерным основаниям, а также в обеспечении сохранности информационных ресурсов.

Информационная сфера России характеризуется активным развитием современных средств информационного обмена и различного типа компьютерных систем. Это создает условия для обеспечения информационной поддержки деятельности аппарата управления на всех уровнях и во всех ветвях власти.

Вместе с тем слабое внимание, уделяемое проблемам обеспечения информационной безопасности, создает объективные условия для незаконного доступа к закрытой информации, ее хищения или разрушения. Особую опасность имеет возможность манипуляций различного рода информацией для негативного воздействия на процесс принятия политических решений[13].

В перечне видов угроз информационной безопасности, обозначенных в Доктрине, стоит обратить особое внимание на:

- вытеснение российских информационных агентств, средств массовой информации с внутреннего информационного рынка и усиление зависимости духовной, экономической и политической сфер общественной жизни России от зарубежных информационных структур;

- манипулирование информацией (дезинформация, сокрытие или искажение информации)[14].

Основными целями защиты от информационно-психологических угроз для России являются:

---

[13] Кирьянов А.Ю. Сущность информационного аспекта национальной безопасности Российской Федерации // Международное публичное и частное право. – 2005. - № 3. – С.42.

[14] Доктрина информационной безопасности Российской Федерации, утверждена Президентом Российской Федерации 09.09.2000 № Пр-1895 // Российская газета. № 187. 2000.

1) Защита от разрушительных информационно-психологических воздействий среды общества, психики населения, социальных групп граждан.

2) Противодействие попыткам манипулирования процессами восприятия информации населением со стороны враждебных России политических сил, проводимых е целью ослабления обороноспособности государства.

3) Отстаивание национальных интересов, целей и ценностей России в информационном пространстве (глобальном, национальном, региональном, субрегиональном, стран СНГ).

4) Постоянное отслеживание отношений российское общества к важнейшим проблемам национальной безопасности (диагностика общественного мнения, психологического состояния нации).

Ведущие страны мира в настоящее время располагают мощным потенциалом информационного противоборства (прежде всего, США, Китай, Израиль, Франция, Великобритания, Германия), который может обеспечить им достижение политических и экономических целей, тем более что отсутствуют международные юридические нормы ведения информационной борьбы.

Для защиты от негативных воздействий социальных объектов в ходе глобальной геополитической информационной борьбы, необходимо создание системы информационно-психологического обеспечения как составной части национальной безопасности России. Данная система должна обеспечить защиту психики политической элиты и населения России от негативного информационно-психологического воздействия (т.е. защите сознания россиян от негативных информационных потоков геополитических противников России). Ее основная задача - обеспечение психологической безопасности политической элиты и населения России.

В Доктрине информационной безопасности Российской Федерации определены следующие основные источники внутренних угроз информационной безопасности:

К внутренним источникам относятся:

- критическое состояние отечественных отраслей промышленности;

- неблагоприятная криминогенная обстановка, сопровождающаяся тенденциями сращивания государственных и криминальных структур в информационной сфере, получения криминальными структурами доступа к конфиденциальной информации, усиления влияния организованной преступности на жизнь общества, снижения степени защищенности законных интересов граждан, общества и государства в информационной сфере;

- недостаточная координация деятельности федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации по формированию и реализации единой государственной политики в области обеспечения информационной безопасности Российской Федерации;

- недостаточная разработанность нормативной правовой базы, регулирующей отношения в информационной сфере, а также недостаточная правоприменительная практика;

- неразвитость институтов гражданского общества и недостаточный государственный контроль за развитием информационного рынка России;

- недостаточное финансирование мероприятий по обеспечению информационной безопасности Российской Федерации;

- недостаточная экономическая мощь государства;

- снижение эффективности системы образования и воспитания, недостаточное количество квалифицированных кадров в области обеспечения информационной безопасности;

- недостаточная активность федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации в информировании общества о своей деятельности, в разъяснении принимаемых решений, в формировании открытых государственных ресурсов и развитии системы доступа к ним граждан;

- отставание России от ведущих стран мира по уровню информатизации федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и органов местного самоуправления, кредитно - финансовой сферы, промышленности, сельского хозяйства, образования, здравоохранения, сферы услуг и быта граждан.

Наибольшую опасность в сфере внутренней политики представляют следующие угрозы информационной безопасности Российской Федерации:

- нарушение конституционных прав и свобод граждан, реализуемых в информационной сфере;

- недостаточное правовое регулирование отношений в области прав различных политических сил на использование средств массовой информации для пропаганды своих идей;

- распространение дезинформации о политике Российской Федерации, деятельности федеральных органов государственной власти, событиях, происходящих в стране и за рубежом;

- деятельность общественных объединений, направленная на насильственное изменение основ конституционного строя и нарушение целостности Российской Федерации, разжигание социальной, расовой, национальной и религиозной вражды, на распространение этих идей в средствах массовой информации.

Из внутренних угроз информационной безопасности Российской Федерации в сфере внешней политики наибольшую опасность представляют:

- информационно - пропагандистская деятельность политических сил, общественных объединений, средств массовой информации и отдельных лиц, искажающая стратегию и тактику внешнеполитической деятельности Российской Федерации;

- недостаточная информированность населения о внешнеполитической деятельности Российской Федерации.

Из внешних угроз информационной безопасности Российской Федерации в сфере внешней политики наибольшую опасность представляют:

- информационное воздействие иностранных политических, экономических, военных и информационных структур на разработку и реализацию стратегии внешней политики Российской Федерации;

- распространение за рубежом дезинформации о внешней политике Российской Федерации;

- нарушение прав российских граждан и юридических лиц в информационной сфере за рубежом;

- попытки несанкционированного доступа к информации и воздействия на информационные ресурсы, информационную инфраструктуру федеральных органов исполнительной власти, реализующих внешнюю политику Российской Федерации, российских представительств и организаций за рубежом, представительств Российской Федерации при международных организациях[15].

На основе национальных интересов РФ в информационной сфере формируются стратегические и текущие задачи внутренней и внешней политики государства по обеспечению информационной безопасности.

Выделяются четыре основные составляющие национальных интересов РФ в информационной сфере.

Первая составляющая национальных интересов РФ в информационной сфере включает в себя соблюдение конституционных прав и свобод человека

[15] Доктрина информационной безопасности Российской Федерации, утверждена Президентом Российской Федерации 09.09.2000 № Пр-1895 // Российская газета. № 187. 2000.

и гражданина в области получения информации и пользования ею, обеспечение духовного обновления России, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны.

Вторая составляющая национальных интересов РФ в информационной сфере представляет собой информационное обеспечение государственной политики РФ, связанное с доведением до российской и международной общественности достоверной информации о государственной политике РФ, ее официальной позиции по социально значимым событиям российской и международной жизни, с обеспечением доступа граждан к открытым государственным информационным ресурсам.

Третья составляющая национальных интересов РФ в информационной сфере состоит в развитии современных информационных технологий, отечественной индустрии информации, в том числе индустрии средств информатизации, телекоммуникации и связи, в обеспечении потребностей внутреннего рынка ее продукцией и выход этой продукции на мировой рынок, а также в обеспечении накопления, сохранности и эффективного использования отечественных информационных ресурсов. В современных условиях только на этой основе можно решать проблемы создания наукоемких технологий, технологического перевооружения промышленности, приумножения достижений отечественной науки и техники. Россия должна занять достойное место среди мировых лидеров микроэлектронной и компьютерной промышленности.

Четвертая составляющая национальных интересов РФ в информационной сфере включает в себя защиту информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем, как уже развернутых, так и создаваемых на территории России[16].

[16] Ковалева Н.Н. Информационное право России: учебное пособие. – М.: Издательско-торговая корпорация «Дашков и К», 2007. – С.234.

По мнению А.Ю. Кирьянова, основными задачами по реализации и защите национальных интересов на современном этапе развития России в информационной сфере являются:

- разработка и принятие долгосрочной программы по обеспечению выхода на уровень ведущих стран мира в области создания систем информатики и управления, основанных на новейших информационных технологиях;

- обеспечение свободы получения и распространения информации гражданами, другими субъектами общественных отношений в интересах формирования гражданского общества, демократического правового государства, развития науки и культуры;

- обеспечение надежной защиты информационного потенциала России (т.е. совокупности информации, обеспечивающей национальные интересы страны; систем ее получения, хранения, переработки и распространения; его субъектов) от неправомерного его использования в ущерб охраняемым законом интересам личности, общества и государства. Осуществление контроля за экспортом из страны интеллектуальной продукции, а также информационных банков данных. Организация эффективной системы подготовки и переподготовки кадров в области обеспечения информационной безопасности;

- развитие взаимодействия государственных и негосударственных систем информационного обеспечения в целях более эффективного использования информационных ресурсов страны;

- совершенствование системы нормативно-правовых актов, регулирующих отношения собственности и соблюдения баланса интересов личности, общества и государства в сфере формирования, хранения и использования информационных ресурсов. Формирование и развитие федеральных и региональных центров сертификации систем информационной защиты и их элементов;

- противодействие целенаправленным действиям по дезинформированию органов власти, населения страны, использованию каналов информационного обмена для нарушения систем управления различными сферами жизнедеятельности государства;

- создание общего информационного пространства стран СНГ в интересах содействия интеграционным процессам, повышения эффективности взаимодействия в реализации общих интересов. Включение России в международную систему информационного обмена с учетом обеспечения российских национальных интересов и противодействия акциями информационной интервенции;

- обеспечение на международном уровне принятия решений о безусловном запрете на использование информационного оружия в мирное время[17].

Далее предлагается сосредоточить внимание на роли государства в области защиты информации. Общие положения по защите информации устанавливает Федеральный закон «Об информации» (ст. 16). Закон рассматривает защиту информации как комплекс «правовых, организационных и технических мер, направленных на:

- обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также ОТ иных неправомерных действий в отношении такой информации;

- соблюдение конфиденциальности информации ограниченного доступа;

- реализацию права на доступ к информации».

Последняя цель, на первый взгляд, не имеет отношения к защите информации. На это не так. Защищать необходимо не только информацию ограниченного доступа, но и открытую информацию, доступ к которой

[17] Кирьянов А.Ю. Сущность информационного аспекта национальной безопасности Российской Федерации // Международное публичное и частное право. – 2005. - № 3. – С.43.

должен быть неограничен. Это также задача государства в отношении информации, предоставляемой для всеобщего сведения органами государственной власти и органами местного самоуправления.

Следующая категория защищаемой информации – эта информация ограниченного доступа, находящаяся в любам режиме конфиденциальности. Но роль государства принципиальна различна в обеспечении различных режимов.

Общедоступную информацию следует защищать от блокирования доступа, уничтожения, модификации (искажения). Информацию ограниченного доступа - от уничтожения, модификации, незаконного копирования, разглашения, незаконного доступа, незаконного использования[18].

Учитывая глобальный характер процессов информатизации и появление международной киберпреступности, мировое сообщество должно иметь межгосударственные организационные структуры но координации работ в области информационной безопасности.

Основным международным органом является Организация Объединенных Наций и созданный ею Совет Безопасности. Эти органы координируют усилия государств по осуществлению мероприятий в области обеспечения информационной безопасности и борьбы с преступлениями в сфере информационных технологий. Спорные вопросы на межгосударственном уровне решает Международный суд.

Система обеспечения информационной безопасности Российской Федерации строится на основе разграничения полномочий органов законодательной, исполнительной и судебной власти федерального уровня, уровня субъектов Российской Федерации, ведомственных структур, а также служб предприятий и организаций[19].

---

[18] Волчинская Е.К. Роль государства в обеспечении информационной безопасности // Информационное право. 2008. № 4. - С.9-16.

[19] Родичев Ю.А. Информационная безопасность: нормативно-правовые аспекты: учебное пособие. – СПб.: Питер, 2008. – С.86-87.

Итак, в связи с новейшими научно-техническими достижениями в области информатики и информационных технологий современное соперничество государств и других объектов социальной природы характеризуется появлением нового фактора - информационного. Через целевое воздействие на информационную среду реализуются угрозы национальной безопасности в различных сферах человеческой деятельности. В политической сфере все большую значимость приобретает информационно-психологическое воздействие с целью формирования отношений в обществе, его реакции на происходящие процессы. В экономической сфере растет уязвимость экономических структур от недостоверности, запаздывания и незаконного использования экономической информации. В военной сфере исход вооруженной борьбы все в большей степени зависит от качества добываемой информации и уровня развития информационных технологий, на которых основываются системы разведки, радиоэлектронной борьбы, управления войсками и высокоточным оружием. В сфере духовной жизни возникает опасность развития в обществе с помощью электронных средств массовой информации агрессивной потребительской идеологии, распространения идей насилия и нетерпимости и других негативных воздействий на сознание и психику человека. Информационная среда, являясь системообразующим фактором во всех видах национальной безопасности (политической, экономической, военной, и др.), в то же время представляет собой самостоятельный объект защиты.

Таким образом, информационная безопасность - защищенность информационной среды личности, общества и государства от преднамеренных и непреднамеренных угроз и воздействий. Обеспечение информационной безопасности Российской Федерации тесно взаимосвязано с решением проблем обеспечения политической, экономической, военной, социальной и других видов национальной безопасности. При этом для обеспечения внешнего аспекта информационной безопасности большая роль

должна отводиться взаимодействию с информационными органами других стран.

Вопросы для обсуждения:

1. Какие проблемы в защите информации можно назвать общенациональными?
2. В чем заключаются интересы общества в поане защиты информации?
3. Какими признаками характеризуется информационная сфера России на современном этапе общественного развития?
4. Какие информационные угрозы можно назвать внутренними для России?
5. Какие информационные угрозы можно назвать внешними для России?

4. Лекция «Проблемы информационной безопасности в период распространения информационных войн»

Целевая группа: политологи, социологи, студенты технических и естественно-научных факультетов

План:

1. Понятие, цели и задачи информационных войн
2. Противостояние информационным атакам

Интернет как отрытая для всеобщего пользования сеть используется не только в законных, но и в противоправных целях. В связи с этим важным является вопрос об обеспечении информационной безопасности в Интернете.

Так, американские теоретики под информационной войной понимают форму агрессивной борьбы сторон, представляющую собой использование специальных методов, способов и средств для воздействия на информационную среду противостоящей стороны и защиты собственной в интересах реализации поставленных целей и задач. В трактовке отечественных ученых, информационная война - это действия, предпринятые для достижения информационного превосходства путем нанесения ущерба информации, процессам, основанным на информации, и информационным системам противника при одновременной защите собственной информации, процессов, основанных на информации, и информационных систем.

В свою очередь, Г.Л.Акопов обозначает информационную войну как активное воздействие на информационную среду противника для достижения поставленных целей и оборону собственного информационного пространства[20].

По мнению С.Е. Чаннова, все правонарушения, совершающиеся в Интернете, можно разделить на две группы:

[20] Акопов Г.Л. Информационное право: учеб. пособие. – Ростов-на-Дону: Феникс, 2008. – С.293.

- традиционные правонарушения, совершаемые с помощью Интернета. Сюда, например, включаются мошенничества при организации Интернет-магазинов, кража средств с пластиковых карт, отмывание денег и т. п.; информационные правонарушения, совершаемые в сети Интернет.

В последней группе можно выделить такие наиболее часто встречающиеся правонарушения, как:

- правонарушения, связанные с незаконным доступом к информации

(«атаки» хакеров на сети различных фирм, иных организаций, личные странички граждан). Совершаются не только с корыстной целью (кража, мошенничество), но и по мотивам личного интереса или желания «показать себя». Тем не менее, практически всегда они наносят ущерб (например, связанный с падением акций пострадавших компаний, распространением конфиденциальной информации и т. п.);

- правонарушения, связанные с повреждением или уничтожением чужой информации, затруднением работы компьютеров совершаются с использованием компьютерных вирусов. В настоящее время в мире насчитывается более 60 тыс. различных вирусных программ и их модификаций[21]. При попадании на чужой компьютер вирус может нанести ущерб как программному обеспечению, так и оборудованию. Вирусы могут использоваться для получения информации и удаленного совершения различных операций, а также как оружие, например в террористических целях. Так, в первый же день войны (2003 г.) с Ираком с помощью информационной атаки через Интернет (отправления по электронной почте, посещения сайта, засылка вирусов и др.) была парализована работа информационного отдела при Президенте США;

- правонарушения, связанные с распространением вредной или ложной информации в Интернете. Эту группу часто называют правонарушениями в

[21] Табунщиков Ю.А. Вопросы защиты информации при использовании Интернет в корпоративных сетях // http://www.crime-research.org/library/Tabun.html

сфере «выражения мнения» (expressions of opinion). Они связаны с распространением через Интернет сведений, порочащих чью-то честь и достоинство; призывов к совершению противоправных действий, конфиденциальной информации; инструкций по изготовлению взрывчатых устройств, производству наркотиков, террористической деятельности; детской порнографии и т. д.;

- правонарушения, связанные с нарушениями законодательства об интеллектуальной собственности.

В рамках второй группы отдельно можно выделить правонарушения, которые не могут существовать в реальном мире и совершаются только в сети Интернет. Сюда можно отнести такие правонарушения, как уже рассматривавшиеся выше кибersквоттинг и тайпосквоттинг, а также распространение спама (электронного мусора)[22].

Среди информационных правонарушений, совершаемых с использованием телекоммуникационных сетей, отдельно выделяют наиболее тяжкие, относимые к информационным преступлениям. Они объединяются под общим названием «киберпреступления». К киберпреступлениям относятся такие общественно опасные деяния, которые совершаются с использованием средств компьютерной техники в отношении информации, обрабатываемой и используемой в Интернете[23].

Очевидно, что уже сегодня мировое сообщество стоит на пороге новой эпохи информационных противоборств, эпохи кибервойн. Кибервойна - информационное противоборство с использованием информационно-коммуникационных компьютерных сетей общего пользования для достижения поставленных целей и задач.

По мнению Г.Л. Акопова, цели и задачи при осуществлении кибервойн преследуются разнообразные, из которых самыми распространенными являются:

---

[22] Чаннов С.Е. Информационное право России. – М.: Приор-Издат, 2007. – С.214-215.
[23] Рассолов И.М. Право и Интернет. – М.: Изд-во Норма, 2009. - С. 257.

- размещение в сети «Интернет» заведомо ложной или провокационной информации для ее последующего распространения в средствах массовой информации и сетевом сообществе;

- манипулирование общественным сознанием, навязывание необходимой идеологии (влияние на общественное мнение);

- вербовка сторонников и рекрутирование единомышленников;

- несанкционированный доступ к информационным ресурсам с последующим их искажением или хищением;

- подрыв международного авторитета государства;

- влияние на принятие политически значимых решений;

- создание атмосферы бездуховности и безнравственности, негативного отношения к культурному наследию;

- дестабилизация политических отношений в обществе;

- распространение компромата и иных сведений, порочащих честь и достоинство политической элиты страны;

- создание атмосферы напряженности между партиями, общественными объединениями и движениями;

- политический либо иной шантаж;

- разжигание межнациональной розни и расовой нетерпимости;

- воздействие на экономическую инфраструктуру государственного образования;

- инициирование массовых беспорядков и иных протестных акций[24].

Наиболее распространенным приемом осуществления политических кибервойн может считаться вброс компромата посредством специализиронанных интернет-сайтов. В сети функционируют целые порталы планомерно вбрасываемого компромата.

Российская политическая элита постоянно сталкивается с информационными угрозами со стороны информационно-

[24] Акопов Г.Л. Информационное право: учеб. пособие. – Ростов-на-Дону: Феникс, 2008. – С. 294.

коммуникационных компьютерных сетей. Существуют в сети ресурсы, дискредитирующие не только политику партий или индивидов, но и политику целых государств, осуществляя тем самым информационные атаки не на те или иные политические институты, а на государственный суверенитет. Так, в сети на протяжении нескольких лет существовал сайт чеченских сепаратистов (kavkaz.org), открыто выступавший не только против проведения контртеррористической операции в Чеченской Республике, но и призывающий бороться против федеральных властей.

Kavkaz.org неоднократно пытались ломать. Самый громкий случай произошел в марте 2002 г. Тогда группа хакеров, скрывающаяся под псевдонимом «Сибирская сетевая бригада», смогла частично ликвидировать сайт. При попытке открыть электронную страницу на экране появлялись сообщения антитеррористической направленности. На следующий день после теракта в ДК на Дубровке пропагандистский сайт был ликвидирован группой российских программистов[25].

Все чаще террористы берут на себя ответственность через интернет-сайты или, что еще хуже, вывешивают на своих сайтах фотографии жертв взрывов и даже видеоролики отснятых терактов. Нередко посредством своих сайтов боевики отчитываются о проделанной работе или обращаются с посланиями к определенной категории граждан. Порой через свои сетевые ресурсы террористы запугивают общественность, угрожая новыми террористическими атаками. Наибольший эффект эти заявления вызывают благодаря массовому цитированию новых сообщений от террористов всевозможными средствами массовой информации[26].

Свободное распространение информации в Интернете не на шутку беспокоит спецслужбы, осознавшие свою слабость перед лавинообразно

---

[25] Утро.ру ежедневная е-газета. Отдел Интернет. 1 ноября 2002 г.

[26] Акопов Г.Л. Правовая информатика: современность и перспективы: учеб. пособие. – Ростов-на-Дону: Феникс, 2005. - С.172.

увеличивающимся потоком информации и, что, не менее важно, дезинформации.

Следует различать информационное противоборство (борьбу) в широком (во всех сферах) и узком смысле слова (в какой-либо сфере, например в политической).

Информационное противоборство (борьба) - форма борьбы сторон, представляющая собой использование специальных (политических, экономических, дипломатических, военных и иных) методов, способов и средств для воздействия на информационную среду противостоящей стороны и защиты собственной в интересах достижения поставленных целей.

Основные сферы ведения информационного противоборства:

- политическая,
- дипломатическая,
- финансово-экономическая,
- военная,
- космическая.

Следует выделить два вида информационного противоборства (борьбы): информационно-техническое и информационно-психологическое.

При информационно-техническом противоборстве главные объекты воздействия и защиты - информационно-технические системы: системы передачи данных (СПД), системы защиты информации (СЗИ) и так далее.

При информационно-психологическом противоборстве главными объектами воздействия и защиты являются:

1. Система принятия политических и экономических решений.
2. Система формирования общественного сознания.
3. Система формирования общественного мнения.
4. Психика политической элиты и населения противостоящих сторон.

Информационное противоборство включает три составные части.

Первая - стратегический анализ, вторая - информационное воздействие, третья - информационное противодействие.

России следует незамедлительно рассмотреть возможность создания специального организационно-управленческого и информационно-аналитического механизма (инструмента), который сможет выполнять организационно-управленческие и информационно-аналитические функции по разработке и проведению информационных операций (оборонительных и наступательных).

Назрела необходимость создания в России системы информационного противоборства, частью которой должна стать внешнеполитическая пропаганда. России для того чтобы выигрывать информационные войны, необходимо создать специальные организационно-управленческие и аналитические структуры для противодействия информационной агрессии против нашей страны.

Так, после начала грузинской агрессии 8 августа 2008 года президент России Д.А. Медведев, прервав отпуск, принимает решение: военной силой прекратить геноцид осетинского народа и принудить грузинское руководство к миру. Для Саакашвили и его заокеанских покровителей действия России стали полной неожиданностью. Ожидали дипломатических заявлений, а в ответ на агрессию против Южной Осетии и убийство российских миротворцев регулярные российские воинские части с тяжелой боевой техникой: танками, гаубицами, системами залпового огня, авиацией - перешли Рокский перевал. Российские войска вошли не только в Южную Осетию, народ которой в августе 2008 года подвергся огню на уничтожение со стороны грузинских вояк, действовавших поистине с жестокостью фашистов, но и в Абхазию, чтобы предотвратить возможность повторения югоосетинской трагедии.

После наказания агрессора в соответствии с нормами международного права, непрерывно наращивается информационное давление на нашу страну,

которая защитила осетинский народ от уничтожения. По сути, в августе 2008 года против России была развернута грязная информационная война. Активное участие в ней принимали, прежде всего, американские и британские СМИ. В материалах CNN, Би-би-си и ряда других СМИ доминировали антироссийские материалы. В США, Великобритании и некоторых других странах усилились попытки негативного формирования образа России.

Агрессивная антироссийская пропаганда пытается навязать мировому сообществу отрицательные информационные клише о России. К сожалению, «пятидневная августовская война» на Кавказе показала нашу несостоятельность в отстаивании своих целей и интересов в мировом информационном пространстве.

Поэтому России в ближайшее время нужно сформулировать и дать адекватный информационный ответ, в первую очередь, на европейском и постсоветском пространстве. Прошедшее после «пятидневной августовской войны» на Кавказе время показало, что пока российская политическая элита пытается сделать соответствующие выводы после информационной агрессии США, Великобритании и ряда других стран против России. Прошло несколько публичных мероприятий с участием ведущих российских экспертов, на которых анализировался ход информационной войны против России (17 сентября 2008 года - организованный Общественной палатой «круглый стол» «Информационная агрессия против России: методы противостояния», 2 октября 2008 года - организованная партией «Справедливая Россия» Международная конференция «Информационные войны в современном мире»).

Главная проблема, которая была очевидной в ходе дискуссий, – это явная недооценка роли информационного противоборства современной российской политической элитой в условиях усиления глобальной экономической и геополитической конкуренции в мире.

После принуждения Грузии и ее заокеанских покровителей к миру геополитическая и геоэкономическая роль России в мире во многом будет определяться тем, сможет ли она создать эффективную систему информационного противоборства. Время требует одновременного создания мощных информационно-аналитических и информационно-пропагандистских структур, предназначенных для реализации информационных моделей урегулирования конфликтов[27].

России необходимо восстановить свой потенциал механизма внешнеполитической пропаганды, который был основательно разрушен в 90-е годы. В этой сфере, как и в сфере ядерных вооружений, к сожалению, произошло одностороннее информационное разоружение. К концу 90-х годов прошлого века, например, на всем африканском континенте не осталось ни одного российского корреспондентского пункта, ни одного представительства отечественных информационных агентств. Сегодня эту «информационную нишу», которую мы покинули после распада СССР, активно заполняет Китай.

Впрочем, отрадно, что провал 90-х годов был осознан российским руководством. С приходом к власти президента В. Путина началось постепенное уверенное восстановление утраченных позиций. Ключевым шагом в этом направлении является создание в 2006 году спутникового телеканала Russia Today. Напомним, что ведущий западный новостной канал CNN был создан в 1980 году. В СССР выделялись огромные деньги на строительство и развитие ракетно-ядерных сил. Однако денег на создание советского спутникового телеканала не нашлось.

Советская политическая элита недооценивала фактор информации. А CNN наращивал свое влияние. Как сказал один американский генерал в 1991 году, во время операции «Буря в пустыне», пока CNN не скажет, что мы выиграли войну, мы ее не выиграли. И это соответствует действительности.

---

[27] Панарин И. Информационные войны - реальный фактор геополитики. Системы информационного противоборства // http://www.centrasia.ru/newsA.php?st=1224016740

Многие сюжеты «победных» действий американских войск были сняты совсем не на поле сражений, а в штате Невада силами специалистов Голливуда, который великолепно умеет имитировать ведение боевых действий. Вспомним хотя бы известный случай с освобождением рядовой Джессики Линч уже во время второй иракской войны в 2003 году. Этот эпизод являлся пропагандистской акцией Пентагона и репетировался заранее, что еще раз демонстрирует всю мощь информационного оружия.

Таким образом, 26 лет отделяют нас от CNN, за годы нашей «информационной спячки» нашли свои ниши Би-би-си и Foxnews, глобальными каналами стали Al Jazzira и Euronews. Сегодня задача, конечно же, заключается в том, чтобы резко увеличить вещание нашего спутникового канала, и, помимо планируемого иновещания на испанском языке, необходимо рассмотреть возможность организации трансляций на китайском языке. С точки зрения выстраивания информационной стратегии необязательно, чтобы вещание на китайском языке велось круглосуточно. Желательно начать вещать хотя бы по два часа в день. Здесь мы можем опередить наших конкурентов. Пока эта ниша пуста, и мы обязаны занять ее первыми.

Кроме того, нужно подумать также о Бразилии и Индии, где мы, обеспечивая наши политические и экономические интересы, должны предоставлять соответствующее информационное сопровождение.

В существенной активизации нуждается латиноамериканское и африканское направления. Создавая в этих регионах информационно-культурные центры и насыщая их соответствующей продукцией, мы обеспечим нашей стране положительный имидж.

Ни в коем случае нельзя забывать и Старый Свет. Сегодня свои экономические интересы обеспечивают информационными средствами различные страны. Интересен в этом плане пример Великобритании, с которой сегодня у нас весьма непростые отношения. Однако в отличие от

РФ, которая по линии МИД выделяет на информационно-культурные и разъяснительные программы около 6,2 млн. долларов США в год, Великобритания на эти цели расходует 862 млн. долларов США. Естественно, что британские интересы в России и других странах мира весьма эффективно прикрываются и защищаются информационно. Так, например, перед нашим великим праздником, Днем Победы, на телеканале НТВ 5 мая 2008 года был очень позитивный репортаж, но не о российской армии и ее достижениях, а о британской. Было детально рассказано о воинских буднях принца Гарри в рядах британской армии, о ее традициях и прочем.

Случайность ли, что как только начинаются какие-то действия российских официальных органов, которые якобы ущемляют британские бизнес-интересы, сразу же появляется волна публикаций о росте авторитаризма в России, нарушении прав человека? Примечательно, что в таких кампаниях участвуют и достаточно авторитетные издания, такие как The Economist, Financial Times. Мы, конечно, не можем заявлять, что эти и другие СМИ получают деньги от правительственных источников, но имеются явные совпадения вала антироссийских публикаций (поводом для которых стали так называемое дело Литвиненко, ситуация вокруг деятельности в РФ Британского совета и др.) с вполне легитимными действиями официальных структур России.

Лучшим ответом, на взгляд И.Панарина, представляется грамотное использование этого опыта для защиты российских национальных интересов. Прежде всего, нам нужно сделать выводы в плане финансирования информационных программ по линии МИД, Росзарубежцентра, а также наших немногочисленных средств информационного противоборства, прежде всего Russia Today и «Голос России».

Внешнеполитический государственный медиахолдинг должен установить конструктивное взаимодействие с каналом Euronews. Вещание на

русском языке этого телеканала, созданного в 1993 году, началось в 2001 году. Сегодня ВГТРК с 16 процентами акций в акционерном капитале компании - один из пяти крупнейших акционеров Euronews, наряду с телекомпаниями Франции, Испании, Италии и Швейцарии.

С учетом того, что Россия в лице ВГТРК - крупнейший акционер и финансовый донор этого канала, необходимо проанализировать весь информационный поток новостей европейского телеканала. Ведь в эфире евроновостей очень мало позитивной информации о России. А во время агрессии Грузии против Южной Осетии по этому телеканалу шли только антироссийские комментарии, порой переходящие рамки приличия (например, 14 августа телеканал показал кадры разрушенного Цхинвала, а строка внизу сообщала, что это разрушенный Гори). Получается, что Россия платит большие деньги, а за это получает нейтральную или негативную информацию о нашей стране, или таковая вообще отсутствует. А ведь по экспертным оценкам в Европе, где Euronews является лидирующим информационным каналом, его смотрят 168 млн. семей, то есть около полумиллиарда зрителей.

Власть России должна умело управлять информационными потоками, наладив конструктивное сотрудничество со СМИ, российскими и зарубежными. Должна быть исключена ситуация 8-11 августа 2008 года, когда даже в новостных программах на российских государственных телеканалах Саакашвили показывали больше, чем лидеров России. За счет заблаговременно подготовленных информационно-пропагандистских операций противнику удалось некоторое время навязывать свои комментарии происходящих событий.

На принципах системности и многоуровневости должна быть построена информационная деятельность российского государства на федеральном, региональном и международном уровнях. Власть должна своевременно, в режиме реального времени предоставлять свои комментарии

к происходящим событиям в мировое информационное пространство. Власть должна уметь эффективно применять преднамеренные утечки государственными структурами в масс-медиа «сенсационной информации». Суть подобной обоюдовыгодной «сделки» заключается в создании посредством подобных публикаций (репортажей) благоприятного имиджа России в мировом информационном пространстве.

Важным аспектом являются необдуманные, нескоординированные, неполные, подверженные двоякому толкованию комментарии происходящих событий, касающиеся конфликтных регионов. В этом случае неподготовленные выступления перед прессой, интервьюирование «на ходу», неопределенность формулировок в конечном итоге осложняют ситуацию, порождают слухи и недоверие к властям. Такая «информационная среда», кроме того, способствует дестабилизации обстановки в стране. Власть должна была заранее разработать и внедрить ряд «домашних заготовок». Ведь конфликты развиваются, как правило, на протяжении длительного периода времени. Суть информационных моделей урегулирования конфликтов должна заключаться в оперативном «вбросе» в СМИ заранее подготовленных комментариев для урегулирования ситуации[28].

С учетом вышеизложенного, предлагаем рассмотреть возможность создания системы противодействия информационным операциям геополитических противников России, включающей ресурсы как государства, так и крупного бизнеса, институтов гражданского общества.

Целесообразно в ответ на усиливающееся информационное давление, – создать государственную систему информационного противоборства с участием крупного бизнеса, которая была бы способна аккумулировать, координировать и направлять все информационные действия. Также нужно резко усилить финансирование программ информационного противоборства. Мероприятия информационного противоборства должны финансироваться

[28] Панарин И. Информационные войны - реальный фактор геополитики. Системы информационного противоборства // http://www.centrasia.ru/newsA.php?st=1224016740

по принципу главного приоритета. Сегодня финансирование программ информационного противоборства более важно, чем финансирование программ ядерного сдерживания. Информационное оружие более опасно для России, чем оружие ядерное. И это необходимо признать политической элите России.

Следует создать частно-государственную систему управления проведением мероприятий информационного противоборства различных уровней: общефедерального, профессионального, группового и индивидуального.

Необходимо начать частно-государственный процесс формирования позитивного имиджа России за рубежом, прежде всего, в Европе. Российский национальный бизнес должен перейти от стратегии покупки футбольных клубов к стратегии покупки крупнейших мировых СМИ для изменения их антироссийской информационной политики.

Необходимо расширить информирование русскоязычного населения всех стран мира. Нельзя ограничивать эту работу только рамками СНГ (хотя наши ближайшие соседи, конечно же, должны быть регионом особого внимания).

Естественно, что каждая страна сама должна вырабатывать шаги для снижения собственных специфических рисков, однако необходимо выработать и дальнейшие международные меры.

Анализ существующих международных политико-правовых документов позволяет предположить, что именно комплексный поход, учитывающий обе концепции (ограничение информационной агрессии, с одной стороны, и минимизация ее последствий - с другой), является наиболее эффективным направлением продолжения международной работы по правовому регулированию в сфере информационного противоборство.

По мнению России, возникает очевидная потребность в международно-правовом регулировании мировых процессов гражданской и военной

информатизации, разработке согласованной международной платформы по проблеме мирного сосуществования в информационном пространстве. При этом российской стороной была предложена модель действий международного сообщества, которая предусматривала дальнейшее рассмотрение ситуации в сфере международной информационной безопасности и принятие Генеральной Ассамблеей ООН новых резолюций, конкретизированных в части ограничения угроз как криминального, так и военного характера.

Россия предлагала, по мере определения общих подходов, вести дело к разработке принципов международной информационной безопасности (режима, кодекса поведения государств), которые могли бы быть первоначально сформулированы в виде многосторонней декларации, а в перспективе - закреплены в форме международно-правового документа. Проработку этих вопросов предлагалось осуществить в рамках женевской Конференции по разоружению.

При этом предполагалось исходить из необходимости принятия таких принципов в комплексе, т.е. применительно как к военной, так и к гражданской сфере. Далее в оценках России излагалось понимание основных угроз и основных задач и целей разработки режима международной информационной безопасности. Кроме того, были предложены терминологические формулировки основных понятий, относящихся к этой проблематике, включая определения собственно международной информационной безопасности, а также «информационной войны» и «информационного оружия».

Все эти основные подходы, понимание угроз, задач международного сообщества и использование терминов впоследствии составили основу предложенного Россией проекта документа «Принципы, касающиеся международной информационной безопасности».

Очевидно, что, если международное сообщество сможет найти общее понимание подходов, изложенных в российском проекте «Принципы международной информационной безопасности», этот документ можно будет рассматривать в качестве концепции, упомянутой в резолюции 55/28, и использовать в дальнейшем как основу многостороннего договора (конвенции), создающего универсальный режим международной информационной безопасности[29].

Проблемы защиты и качества информации также учитываются в отечественном праве. Так ст. 29 Конституции РФ гласит: «2. Не допускается пропаганда или агитация, возбуждающие социальную, расовую, национальную или религиозную ненависть и вражду. Запрещается пропаганда социального, расового, национального, религиозного или языкового превосходства». Однако все вышеизложенное в современных компьютерных сетях можно встретить в изобилии.

Примечателен тот факт, что ответственность за распространение недоброкачественной информации, за нарушение порядка распространения информации регулируется не только Конституцией РФ, но и предусматривается нормами УК РФ[30]. Прежде всего это клевета (ст. 129), оскорбление (ст. 130), воспрепятствование законной профессиональной деятельности журналистов (ст. 144), заведомо ложная реклама (ст. 182), заведомо ложное сообщение об акте терроризма (ст. 207), сокрытие информации об обстоятельствах, создающих опасность для жизни или здоровья людей (ст. 237), незаконное распространение порнографических материалов или предметов (ст. 242), публичные призывы к насильственному изменению конституционного строя РФ (ст. 280), возбуждение

---

[29] Горбенко А.Н. Правовое регулирование в сфере информационного противоборства // Информационное право. – 2008. - № 3 (14). - С.25-26.

[30] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (в ред. от 25.11.2008) // Собрание законодательства РФ. 17.06.1996. № 25. Ст. 2954.

национальной, расовой или религиозной вражды (ст. 282), публичные призывы к развязыванию агрессивной войны (ст. 354)[31].

Так, по мнению В.А. Копылова, борьба с правонарушениями в Интернет должна быть направлена на защиту:

- национальной безопасности (например, от распространения инструкций по изготовлению взрывчатых устройств, производству наркотиков, террористической деятельности, призывами к свержению власти);

- несовершеннолетних (оскорбительные формы маркетинга, насилие и порнография);

- человеческого достоинства (расовая дискриминация и расистские оскорбления);

- информации и информационных ресурсов (например, от неправомерного доступа, злонамеренного хакерства и т.п.);

- тайны личной жизни (несанкционированный доступ к персональным данным, электронные оскорбления);

- репутации («навешивание ярлыков», незаконная сравнительная реклама);

- интеллектуальной собственности (несанкционированное распространение защищенных авторским правом работ, например, программного обеспечения, музыки, неправомерное использование торговых марок в качестве доменных имен и т.п.).

Можно выделить следующие основные направления правового регулирования отношений в Интернет:

- защита от вредной и незаконной информации (содержания);

- соблюдение авторских и смежных прав в условиях распространения информации в электронной форме и технически легкого копирования такой информации;

---

[31] Акопов Г.Л. Правовая информатика: современность и перспективы: учеб. пособие. – Ростов-на-Дону: Феникс, 2005. – С.191.

- вопросы электронного документооборота, доменные имена, правовое регулирование отношений при использовании электронной цифровой подписи;

- вопросы киберэкономики (электронные деньги, реклама, маркетинг, электронные публикации, электронные контракты, налог на передачу информации, ЭЦП - см., например, ст. 160, п. 2. ст. 434, п. 3. ст. 847 ГК РФ);

- информационная безопасность как состояние защищенности всех объектов информационных правоотношений в Интернет;

- правонарушения в Интернет.

При правовом регулировании отношений в Интернет важно соблюдение баланса:

- между свободой слова и интересами несовершеннолетних. Например, любые действия по защите несовершеннолетних не должны принимать формы безусловного заперта на использование Интернет для распространения содержания, доступного с помощью иных средств;

- свободы доступа к информации и информационной безопасностью личности, общества, государства. Защита государственной тайны, коммерческой тайны, других видов тайн не должна накладывать запрет на распространение и свободный доступ к информации, затрагивающие свободы и права человека и гражданина;

- свободы производства информации и ограничения производства и распространения опасной информации, информации, оскорбляющей личность. Свобода - не вседозволенность.

Потребители имеют все больший доступ к онлайновым банковским операциям, каталогам и прочим услугам. Оплачиваться услуги могут как традиционными методами, так и электронными с использованием «электронных денег». Системы электронных денег разрабатывают несколько компаний. Сами электронные деньги - эквивалент банковского депозита,

либо выданный в виде зашифрованной серии цифр компьютерным сетям, либо записанный на карточку со встроенным микропроцессором.

Важной вехой на пути формирования основ информационного общества на международном уровне следует считать принятие в Окинаве Хартии Глобального информационного общества, в которой устанавливаются основные принципы вхождения мирового сообщества в такое общество на основе единой информационной инфраструктуры, базис которой составляет Интернет.

Таким образом, правовое регулирование отношений в Интернет может базироваться на основе норм актов информационного законодательства. Можно выделить основные направления этого законодательства, имеющие наиболее тесную связь с отношениями, возникающими в Интернет, многие из которых могут быть трансформированы для распространения их действия и на виртуальную среду. Это следующие направления:

- законодательство об осуществлении права на поиск, получение и потребление информации (о праве на доступ к информации или право знать);

- законодательство об интеллектуальной собственности (законодательство об авторском праве и смежных правах, патентное законодательство, законодательство о ноу-хау);

- законодательство о СМИ;

- законодательство о документированной информации и об информационных ресурсах;

- законодательство об информации ограниченного доступа;

- законодательство о создании и применении информационных систем, информационных технологий и средств их обеспечения;

- законодательство об ответственности за правонарушения в информационной сфере.

Именно нормы актов этих направлений могут быть рассмотрены на предмет дополнений и изменений для приведения в соответствие с особенностями среды Интернет[32].

К сожалению, в Российской Федерации адекватные средства борьбы с Интернет-правонарушениями в большинстве случаев отсутствуют. Так, например, можно говорить только «о существовании подхода к подготовке» проекта закона о спаме. Поэтому в основном можно опираться лишь на зарубежный опыт правового регулирования в этой сфере.

Так, первым международным соглашением по юридическим и процедурным аспектам расследования и криминального преследования киберпреступлений стала Конвенция о киберпреступности, принятая Советом Европы 23 ноября 2001 г.[33]. Конвенцией предусматриваются скоординированные на национальном и межгосударственном уровнях действия, направленные на недопущение несанкционированного вмешательства в работу компьютерных систем.

Помимо конвенции страны Европы разрабатывают и иные законодательные инициативы, призванные оградить государства от компьютерных преступлений. Так, к закону 1990 г., который регулировал борьбу с компьютерными преступлениями, в Великобритании разрабатывается исправление. Старая формулировка уже не отражает все нюансы, за которые хакеры должны понести наказание. В связи с этим в закон будет внесена поправка, согласно которой к хакерам будут применяться жесткие меры наказания, вплоть до тюремного заключения. В поправку будут включены такие действия, как атаки, которые подрывают работу сетей и выводят их на длительное время из строя. Поправка предусмотрит законное разрешение таких проблем, как компьютерные преступления, а также кражи баз данных.

---

[32] Копылов В.А. Информационное право: учебник. – М.: Юристъ, 2005. – С.248-249.

[33] Convention on Cybercrime (Budapest, 23.XI.2001) // http://www.crime-research . org/library/cybercrime-convention, doc

Противостоять действиям хакеров, как известно, можно законодательными и техническими методами. Именно на последние сделали ставку крупнейшие мировые провайдеры. 28 марта 2005 г. крупнейшие провайдеры интернет-услуг объявили о заключении глобального антихакерского альянса. В его рамках компании создадут систему раннего оповещения об атаках компьютерных злоумышленников в Интернете.

Как сообщило 28 марта агентство Dow Jones, в антихакерский альянс войдут 18 крупнейших провайдеров со всего мира, включая BT Group, Deutsche Telekom, MCI, NTT Communications, Cisco Systems и EarthLink. Объединиться конкурирующих участников рынка заставила общая беда - разгул компьютерного «терроризма»[34].

Средства борьбы с Интернет-правонарушениями можно разделить на организационно-технические и юридические. В качестве примера первых можно назвать множество технологий, которые позволяют контролировать содержание, доступное в Интернете. Фильтрующее программное обеспечение представлено тремя видами: «черные списки» (блокирует доступ к включенным в список источникам), «белые списки» (доступ возможен только к перечисленным источникам), «нейтральная маркировка» (установление рейтингов, согласно которым пользователь сам решает вопрос о доступе к помеченному содержанию)[35].

Одним из средств защиты являются также «Блокираторы поведения», которые следят за компонентами операционной системы, исполняемыми кодами и командами, поступающими на узел с электронной почтой, файлами из Интернета и из других сетей. Обнаруженные сомнительные коды, команды блокираторы изолируют, ограничивая их доступ к другим узлам и распространение по сети. Широкое распространение имеют и программные

[34] Захаров Д. С хакерами поборются всем миром. // ИД «Коммерсантъ». 29.03.2005.
[35] Чаннов С.Е. Информационное право России. – М.: Приор-Издат, 2007. – С.216.

антивирусные комплексы, такие, как AVP - Касперского, Россия, Norton Antivirus США и др.[36]

В некоторых европейских странах приняты или предлагаются к принятию законы, которые позволяют привлечь провайдеров хостовых услуг к юридической ответственности за расположенное на их компьютере содержание, если они предположительно знали, что предлагаемое содержание незаконно, или не предприняли меры для его устранения, когда их внимание обратили на эти факты.

Уже имеется несколько примеров юридических средств борьбы с Интернет-правонарушениями, когда провайдеры доступа в Интернет привлекались к ответственности в суде. В Германии проводилось расследование против компаний CompuServe и Deutsche Telecom AG T-Online, которые предоставляли доступ к неонацистской «домашней странице» в Канаде. Провайдеры были обязаны блокировать доступ к этой информации[37].

В Турции уже принят закон, в соответствии с которым за диффамацию или публикацию в Интернете заведомо ложной информации суд может наложить на ее авторов (а заодно - и на Интернет-провайдеров) штраф до 195 тыс. долл.

В последние годы в США предпринимаются значительные усилия по борьбы со спамом. Так, закон штата Калифорния обязывает рассылающих непрошеные сообщения приводить в письме действующий обратный адрес электронной почты либо телефон, по которому пользователи могут выразить свое нежелание далее получать такого рода сообщения. На само письмо также накладываются ограничения: перед темой письма обязательно должна стоять аббревиатура «ADV:» либо в случае порно-спама – «ADV:ADLT».

---

[36] Табунщиков Ю.А. Вопросы защиты информации при использовании Интернет в корпоративных сетях // http://www.crime-research.org/library/Tabun.html

[37] Табунщиков Ю.А. Вопросы защиты информации при использовании Интернет в корпоративных сетях // http://www.crime-research.org/library/Tabun.html

Нарушение данного закона на территории штата Калифорния считается преступлением[38].

В соответствии с федеральным законодательством за каждое письмо, попадающее под категорию несанкционированной почты, судом может быть наложен штраф от 500 до 50 тыс. долл. Чтобы коммерческая рассылка не попадала под данную категорию, в письме должен быть четко указан отправитель, а получателю предоставлена возможность легко удалять себя из списков рассылки. При этом важно, чтобы отписаться можно было на самом деле. Если спаммер выполняет эти условия, его действия будут расценены как реклама, а не как рассылка спама. Федеральная комиссия связи (FCC) тоже сможет предпринимать карательные меры к спаммерам, на которых поступают жалобы от пользователей и Интернет-провайдеров[39].

Итак, компьютерная преступность и кибертерроризм представляют особую общественную национальную и международную опасность. Поэтому необходима четкая и последовательная международная политика по противостоянию кибертеррору, нужна высококвалифицированная разведка.

Профилактика и сдерживание киберпреступности и кибертерроризма – это комплексная проблема. Сегодня законы должны соответствовать требованиям, предъявляемым современным уровнем развития технологий. С этой целью необходимо проводить целенаправленную работу по унификации и совершенствованию национальных законодательств, регулирующих распространение информации в телекоммуникационных сетях общего пользования.

Однако борьба с компьютерными преступлениями не должна ограничиваться нормотворчеством. Об этом, в частности, велась речь на заседании Совета Безопасности Российской Федерации по вопросу развития информационного общества в России. По итогам заседания Сергей Иванов, объясняя рассмотрение стратегии без присутствия журналистов, отметил, что

---

[38] http://www.mdi.ni/aspnews/body/08.01.2002_40196.html

[39] Чаннов С.Е. Информационное право России. – М.: Приор-Издат, 2007. – С.217.

с точки зрения национальной безопасности «есть определенный сегмент информационной безопасности, который присутствует в любой развитой стране». После чего отметил: «Нам надо бороться с кибертерроризмом»[40].

Поэтому также приоритетным направлением является организация взаимодействия и координации усилий правоохранительных органов, спецслужб, судебной системы, обеспечение их необходимой материально-технической базой[41].

Поскольку компьютерный терроризм – уже реальность сегодняшнего дня, необходимо закрепить на законодательном уровне обязанность государственных и частных структур по принятию технических мер, обеспечивающих защиту компьютерных сетей, как одного из наиболее уязвимых элементов современного общества.

Вопросы для обсуждения:

1. Дает ли Интернет возможности для распространения террористической информации и в чем это выражается?
2. Встречались ли Вы в Интернете с информацией пропагандирующей террористические идеи? В каких формах это выражается, с чем чаще всего это связано?
3. Какой международный опыт можно использовать для обеспечения безопасности информации?
4. Какие существуют средства борьбы с информационными нарушителями? Какие из них, по Вашему мнению, эффективны, а какие нет?
5. Информационные войны: это миф или реальность? Есть ли надежные средства защиты в такой волне?

---

[40] Совбез РФ утвердил стратегию развития информационного общества. 25.07.2007. РИА Новости, http://www.rian.ru/politics/ 20070725/69671890.html .

[41] Голубев В.А. Кибертерроризм - понятие, терминология, противодействие. // http://www.crime-research.ru/. 09.08.2004.

5. Лекция «Особенности влияния материалов экстремисткой и террористической направленности на молодежную аудиторию: экспертиза информации и способы противодействия»

Целевая группа: сотрудники АТК, силовых ведомств, профессиональные психологи, социологи, регионоведы

План:

1) Проявления экстремизма как объект научного исследования.

2) Социальные, правовые и психологические аспекты изучения субъектов и объектов экстремистской деятельности.

3) Экстремистская направленность как психологическое понятие.

4) Технологии противодействия влиянию информации экстремисткой направленности.

5) Технологии убеждающего воздействия.

6) Рекомендации.

Актуальность темы данной лекции обусловлена проблемой создания системы противодействия терроризму и экстремизму в России. В настоящий момент терроризм и экстремизм являются крайней формой социальной неприязни, проблема которой не является новой и неоднократно озвучивалась авторами в разных областях науки и практики.

В рамках судебно-психологических экспертиз (СПЭ), как направления в применении специальных познаний для разрешения вопросов по конкретному делу в предварительном, либо судебном следствии (Л.В. Алексеева, И.А Горьковая, В.Ф. Енгалычев, Л.П. Конышева, М.М. Коченов, И.А. Кудрявцев, А.Р. Ратинов, Ф.С. Сафуанов, Т.В. Сахнова, Т.Н. Секераж, О.Д. Ситковская, Е.Н. Холопова, С.С. Шипшин, А.Л. Южанинова и др.), многие на практике уже встретились с необходимостью оценки материалов по статьям 280 УК РФ «Публичные призывы к осуществлению экстремистской деятельности» и 282 УК РФ «Возбуждение ненависти либо

вражды, а равно унижение человеческого достоинства». При том, что частота заказов на такого рода исследования со стороны правоохранительных органов, государственных и частных организаций, растёт, методология судебной психологической экспертизы материалов экстремистской направленности на настоящий момент поступают крайне редко. Списки признаков, которыми руководствуются эксперты, как правило, созданы на основании прецедентов и потому не являются исчерпывающими, либо, наоборот, избыточны, зачастую пересекаются и дублируют друг друга. Это обусловлено тем, что содержание влияния материалов экстремистской направленности на аудиторию не раскрыто и экспериментально не изучено.

Возбуждение вражды может быть обусловлено не только призывами (являющимися, скорее, предметом лингвистического исследования), после чего оно объясняется через феномен установки, как ведущей формы создания механизма разжигания социальной розни. В случае, если потребность проявляется в ситуации, делающей возможным её удовлетворение, в субъекте возникает «конкретно очерченная установка» и он, по замечанию Д.Н. Узнадзе, «чувствует в себе импульс к деятельности в совершенно определённом направлении». Как итог, наличие *потребности* и *ситуации* является обязательным условием формирования определённой установки. Г.М. Андреева говорит о трёхкомпонентности социальной установки: под *когнитивной* составляющей понимаются знания о некотором феномене, взаимодействие с которым регулирует установка, под *аффективной* – отношение к нему, под *конативной* – непосредственное побуждение к действию. А.Г. Асмолов указывает, что установка определяет устойчивый характер протекания деятельности, освобождает субъекта от необходимости принимать решения и может выступать в качестве фактора, обусловливающего инерционность, косность динамики деятельности и затрудняющего приспособление к новым ситуациям. В связи с этим важно

выявить, действительно ли материалы экстремистской направленности актуализируют негативные аттитюды.

Чтобы помочь суду в установлении факта, является ли публикация конкретных материалов экстремистской деятельностью, необходимо раскрыть психологическую составляющую воздействия автора на аудиторию. Поэтому необходимым условием является определение судебно-психологического экспертного понятия *экстремистской деятельности*. Под ней подразумевается активность, направленная на деструктивное воздействие на социум, проявляющаяся в первую очередь в преступлениях по мотивам расовой, национальной, религиозной и иной социальной вражды и ненависти.

В современном российском законодательстве по вопросам экстремистской деятельности рассматриваются термины «разжигание», «возбуждение», «вражда», «ненависть», «неприязнь», «рознь». На основании анализа выделяется *социальная неприязнь* – комплексное понятие, обозначающее негативные установки в отношении любых социальных групп. Показывается, что только оно включает в себя все компоненты установки и не является чересчур широким в отличие от всех остальных и потому является предметом юридико-психологическое изучения.

Эксперт-психолог может дать заключение о том, обладают ли определённые материалы экстремистской направленностью (есть ли призывы к террористической или экстремисткой деятельности), что является важным для принятия судом решения по конкретному делу. Следствие может признать, что их публикация является преступлением, а может и посчитать её законной даже при утвердительном ответе об экстремистской направленности данных материалов (например, при публикации примера в учебнике для экспертов или следователей).

На основании обзора исследований, посвящённых социальной напряжённости за последние годы, а также уголовных дел, материалов

судебных экспертиз (в основном психологических, лингвистических и психолого-лингвистических), было выделено шесть базовых причин её формирования (субъективная сторона данного преступления). Возможно продолжение списка, однако остальные факторы, также влияющие на возникновение социальных конфликтов либо просто коррелируют с указанными нами феноменами, т.е. опосредованно воздействуют на социум, либо являются следствием элементов этого списка. Всего их выделено шесть:

- усиление миграционных процессов;
- конкуренция на рынке труда;
- ухудшение условий жизни;
- криминальный фактор;
- потребность во включении в соответствующую субкультуру;
- теснота контакта с более экономически эффективным социумом.

В рамках раскрытия объективной стороны данного преступления должны быть проанализированы общенаучные и частно-психологические подходы к *«пропаганде»*, под которой понимается психологическое воздействие на аудиторию, ведущееся специальными методами, с целью распространения каких-либо идей, взглядов, представлений и побуждений к действиям, а также формирования у людей определенных установок, целей, мотивов поведения. Анализируя вышеперечисленные определения, можно сделать вывод, что основными элементами процесса пропаганды являются: её субъект (социальная группа, интересы которой выражает пропаганда); объект (аудитория или социальные общности, которым адресована пропаганда); формы и методы; содержание (текстовый или иной эквивалент); средства и каналы пропаганды.

К таким каналам пропаганды, как печать, радио, телевидение и публичные выступления, выделенным А.Р. Ратиновым и М.В. Крозом, добавляется ещё один – *информационные сети (Интернет)*, которые представляют собой совокупность всех вышеперечисленных СМИ, т.к.

позволяют оперировать печатной, аудиальной, визуальной и иной информацией. В их отношении выделяются и раскрываются такие особенности, как лёгкий доступ, активность, групповой характер, мультимедийность, открытость и обширность, анонимность.

Пропаганда рассматривается как совокупность двух составляющих: убеждения и внушения. Обязательным условием убеждения является строгое следование правилам логики, поскольку оно апеллирует к рациональному мышлению субъекта, его разуму. В основе внушения же лежит ослабление действия сознательного контроля, осуществляемого индивидом в отношении воспринимаемой информации.

Создание установок у аудитории само по себе не является достаточным для того, чтобы влияние привело к нужному автору результату. Для этого *формирование* установок негативного характера должно на практике сопровождаться *подкреплением*. Два данных направления деятельности чаще встречаются в едином комплексе, однако в ряде случаев могут быть разделены и соответствовать *прямой пропаганде* и *косвенной пропаганде*.

Прямая пропаганда – создание определённых установок у аудитории. *Косвенная пропаганда* – подкрепление уже существующих у аудитории установок. В этом смысле она возможна как совместно с прямой (наиболее распространённый вариант), так и отдельно (причём в двух вариантах).

Первый: аудитория не обладает образами, которые подкрепляет автор. Косвенная пропаганда будет только дополнением к прямой.

Второй вариант: аудитория уже обладает искомыми образами, установлены связи между образами определённых групп и образами действий. Воздействие, оказываемое автором, усиливает эти связи, увеличивает интенсивность установки, актуализацию потребностей, входящей в её состав. В итоге воздействие актуализирует ксенофобские установки.

Выявление границ аудитории является важным для определения, имеются ли у неё искомые установки и потому должно включаться в исследовательскую часть работы эксперта.

Чаще всего на практике встречается одновременное осуществление прямой и косвенной пропаганды экстремизма. В связи с комплексностью его структуры данный вид обозначается как *комплексная пропаганда*.

К судебным экспертизам материалов экстремистской направленности можно выделить несколько подходов: психологический (А.Р. Ратинов, М.В. Кроз, Н.А. Ратинова и др.), лингвистический (Е.И Галяшина, М.А. Осадчий и др.), психолингвистический (А.А. Леонтьев, В.И. Батов и др.), социогуманитарный (Н.М. Гиренко). В настоящее время экспертное изучение материалов на наличие признаков экстремизма чаще всего носит комплексный психолого-лингвистический характер. Указанные подходы были обобщены в табличной форме (Таблица).

Таблица Объекты и предметы лингвистики, психолингвистики и психологии

	Лингвистика	**Психолингвистика**	**Психология**
Объект	1. Система языковых знаков. 2. Совокупность речевых событий или речевых ситуаций.	1. Процессы порождения и восприятия речи. 2.Процессы кодирования и декодирования в индивидуальных участниках коммуникации. 3. Совокупность речевых событий или речевых ситуаций.	1. Психика в закономерностях её развития как свойство высокоорганизованной материи. 2. Человек как носитель высокоразвитой психики. 3. Психическая деятельность, взятая в совокупности и единстве.
Предмет	1. Система языковых средств, используемых в коммуникации. 2. Исследование взаимосвязей форм языка внутри самого языка, не касаясь вопросов отношения к его носителю, то есть человеку.	1.Процесс функционирования знаковой системы – процесс создания и восприятия знаков языка людьми. 2.Процессы производства и восприятия речи в их соотнесённости с физиологическим и психическим состоянием участников коммуникации. 3.Влияние ситуации общения на сообщения. 4. Отношение между системой языка и языковой способностью. 5.Связь между содержанием, мотивом, формой речевой деятельности и структурой, элементами языка.	1. Процесс, деятельность как основной способ существования психического; психические процессы и психические образования. 2. Факты, закономерности развития и механизмы психики; порождении, функционирование и строение психического отражения реальности. 3. Порождение, функционирование и строение механизма отражения реальности.

Проведенный анализ позволяет выявить признаки информации, которая содержит призывы к террористической и экстремисткой деятельности:

- материалы террористической и экстремистской направленности – это материалы, содержащие пропаганду политической, идеологической, расовой, национальной или религиозной ненависти или вражды либо ненависти или вражды в отношении какой-либо социальной группы;

- эти материалы обусловливают изменение эмоционального состояния, понижение уровня выраженности таких состояний, как «радостное, «солнечное» настроение», «благодушие», «легкая эйфория», «комфорт», «весёлый», «хорошее настроение», «счастливый», «жизнерадостный», восторженный», «радостный», «оптимистичный», «расслабленный», «равнодушный», «спокойный», «полный надежд», «довольный» и повышение таких, как «печаль», «тоскливость», «грусть», «плохое настроение», «несчастный», «мрачный», «унылый», «печальный», «разочарованный», «пессимистичный»;

- материалы экстремистской направленности актуализируют негативные установки к определённым обобщённым группам у аудитории при их наличии;

- материалы экстремистской направленности обусловливают изменение отношения к определённым обобщённым социальным группам на более негативное при комплексной пропаганде экстремизма, либо косвенной – в отношении групп, обладающих выраженными интолерантными установками. На не обладающих таковыми косвенная пропаганда такого влияния не оказывает;

- материалы экстремистской направленности обусловливают проявления агрессии, в том числе открытой, в первую очередь, за счёт понижения механизмов приспосабливаемости к конфликтным ситуациям как у лиц, обладающих выраженными интолерантными установками, так и у остальных;

- материалы экстремистской направленности не просто повышают уровень интолерантности человека, а формируют негативное отношение и агрессивные установки в отношении конкретных социальных групп.

Материалы экстремистской направленности могут провоцировать социальную неприязнь в обществе вне зависимости от первоначальных мотивов их создания, либо распространения, и законодатель должен ограничить влияние подобных материалов на аудиторию. Для правового контекста важна объективная направленность – то, какие цели реально достигаются в социуме конкретным действием (например – публикацией материалов). При этом цели деятельности автора и публикующего материалы могут быть совершенно другими, не имеющими к экстремизму прямого отношения. Направленность, в свою очередь, можно определить по тому эффекту, который вызывает знакомство с материалом у аудитории. И здесь особенно важно участие психолога – лингвист и психолингвист имеют дело с источником информации, и лишь психолог – с её приёмником – аудиторией.

Как противостоять воздействию информации террористической и экстремисткой направленности? Это сложный и многоаспектный процесс, однако, с точки зрения тех наук, которые исследуют информационные каналы воздействия на ценностную сферу человека в основе такого противодействия должны рассматриваться смыслотехнологии убеждающего воздействия. Для того, чтобы государство и общество могло противостоять тем негативным влияниям, которые в настоящее время все более и более агрессивно воздействуют на подростков и юношей, необходимо разрабатывать технологии воздействия, ориентированные на убеждающий эффект. В мировой и отечественной практике такие технологии есть (например – эмоциональный резонанс, социальная индукция, фиксация на авторитетах и т. д.). Они зарекомендовали себя как результативные в плане формирования ценностно-смысловых ориентаций подрастающего поколения. Это позитивный педагогический и психотерапевтический опыт, опыт работы

ряда общественных организаций и профессиональных сообществ и, к сожалению, это зачастую опыт тех, кто распространяет идеи расовой нетерпимости, установки катастрофизации, формирует «ореол героя» вокруг участников террористических актов.

Чтобы перевести убеждающую информацию, являющуюся пока ценностью лишь для транслятора государственных и общественных ценностей, в личностно значимую и для молодого человека, последнему необходимо показать, что основанные на этой информации действия и поступки не только не будут противоречить его ценностным ориентациям, но и будут способствовать удовлетворению его определенных потребностей и соответствовать его ценностным ожиданиям.

В процессе использования технологий убеждающих воздействий происходит нивелирование отчуждения личности молодого человека от постигаемого содержания. Этот результат может быть достигнут в процессе направленного воздействия со стороны транслятора, использующего ценностно-смысловые затруднения в качестве задач на выявление смысла или задач на различение смыслов как преодоление ценностно-смысловых барьеров, без решения которых каждый человек начинает ощущать конфликтность или двойственность ситуации. В ходе решения «задачи на смысл», преодоления ценностно-смысловых барьеров и формирования позитивного ожидания в принятии осваиваемого содержания происходит внутренняя работа личности по соотнесению проявлений мотива в нескольких пересекающихся друг с другом плоскостях: в отношении мотива к преодолеваемым личностью ради его достижения внешним и внутренним преградам; по сопоставлению мотива с другими выступающими в сознании субъекта возможными мотивами той же деятельности; по оцениванию мотива в его отношении к принятым личностью нормам и идеалам; по соотнесению мотива с реальными с точки зрения личности ее возможностями, т.е. с воспринимаемым образом Я; по сравнению

собственного мотива с предполагаемыми мотивами других субъектов. В качестве технологий направленного воздействия убеждающего характера могут быть выделены следующие технологии:

- прямое воздействие на ценностно-смысловую сферу личности;

- использование идентичности с целью формирования заданного отношения к конкретному объекту;

- использование стимульной (в частности, соревновательной) мотивации как фактора формирования определенных смыслов через конвенцию.

Ориентируясь на особенности организации смыслопоисковой активности человека как условие осмысления жизненного опыта (Р.Р. Каракозов), закономерности смысловых координаций, трансформаций смыслов в совместной деятельности и направленной трансляции смыслов в обучении (Д.А. Леонтьев), особенности механизмов психотехники выбора (Ф.Е. Василюк), технологии смыслодиактического воздействия (Абакумова И.В., Ермаков П.Н.), был разработан процессуальный компонент убеждающих воздействий, и в результате эта технология была ориентирована непосредственно на механизмы смыслообразования. Процессуальный компонент придает определенный вектор наиболее смылонасыщенным компонентам постигаемого содержания и выводит их смыслообразующий потенциал на уровень раскристаллизации смыслов самого познающего. Процессуальный вектор имеет два достаточно выраженных направления – культурализация (направленность на раскрытие смысловых пульсаров постигаемого содержания как носителя «кристаллизованного» смысла и смыслообразующего контекста) и персонализация (направленность на раскрытие интроспективных смысловых потенций самого постигающего).

На уровне реализации технологии убеждающих воздействий в практике мы исходили из непосредственных механизмов смыслообразования в контексте формирования ценностей антитеррористического мышления. Это

уровень раскристаллизации смыслов, сбрасывания ими текстовой, знаковой формы. Субъективный опыт постигающего информацию, замкнувшись на объективных значениях или объективированных смыслах, характеризуется смысловым приращением, динамика которого и может быть названа продуктом убеждения – ценностным приращением.

На начальном этапе предлагается формирование установки. Установка – готовность, предрасположенность субъекта, возникающая при предвосхищении им появления определенного объекта и обеспечивающая устойчивый целенаправленный характер протекания деятельности по отношению к данному объекту. Понятие установки первоначально было введено в экспериментальной психологии немецкими психологами для обозначения обусловленного прошлым опытом фактора готовности действовать тем или иным образом, определяющего скорость реагирования на воспринимаемую ситуацию и некоторые иллюзии восприятия (Г. Мюллер, Т. Шуман), а также для описания, возникающего при постановке задачи неосознаваемого состояния готовности, обусловливающего направленность различных психических процессов. Позднее понятие социальной установки аттитюда вводится в социальную психологию и социологию для обозначения субъективных ориентаций индивидов как членов группы (или общества) на те или иные ценности, предписывающих индивидам определенные социально принятые способы поведения (У. Томас, Ф. Знанецкий). В качестве объяснительного принципа изучения психических явлений установки наиболее глубоко разработана Д.Н. Узнадзе и его школой. В общей психологии установка применяется при исследовании целенаправленного поведения животных, психофизиологических механизмов приспособления организма к предвосхищаемым ситуациям, избирательности и направленности психических процессов, механизмов неосознаваемой регуляции деятельности личности, формирования характера. В социальной психологии установка используется при изучении отношений личности как

члена группы к тем или иным социальным объектам, механизмов саморегуляции, устойчивости и согласованности социального поведения, процесса самореализации и изменения установки, например, под влиянием пропаганды, а также при прогнозировании возможных форм поведения личности в определенных ситуациях.

Функция установки, ее эффекты и содержание раскрываются при изучении ее роли в регуляции деятельности. Основные функции установки в деятельности: а) установка определяет устойчивый, последовательный, целенаправленный характер протекания деятельности, выступает как механизм ее стабилизации, позволяющий сохранить ее направленность в непрерывно изменяющихся ситуациях; б) установка освобождает субъекта от необходимости принимать решения и произвольно контролировать протекание деятельности в стандартных, ранее встречавшихся ситуациях; в) установка может выступить и в качестве фактора, обусловливающего инертность, косность деятельности и затрудняющего приспособление субъекта к новым ситуациям. Эффекты установки непосредственно обнаруживаются только при изменении условий протекания деятельности. Вследствие этого общим методическим приемом изучения феноменов установки является прием «прерывания» деятельности. Содержание установки зависит от места объективного фактора, вызывающего эту установку, в структуре деятельности. В зависимости от того, на какой объективный фактор деятельности направлена установка (мотив, цель, условие деятельности), выделяются три иерархических уровня регуляции деятельности — уровни смысловых, целевых и операциональных установок. Смысловая установка выражает проявляющееся в деятельности личности отношение ее к тем объектам, которые имеют личностный смысл. По происхождению смысловые установки личности производны от социальных установкок.

Смысловые установки содержат информационный компонент (взгляды человека на мир и образ того, к чему человек стремится), эмоционально-оценочный компонент (антипатии и симпатии по отношению к значимым объектам), поведенческий компонент (готовность действовать по отношению к объекту, имеющему личностный смысл). С помощью смысловых установок индивид приобщается к системе норм и ценностей данной социальной среды (инструментальная функция), они помогают сохранить статус-кво личности в напряженных ситуациях (функция самозащиты), способствуют самоутверждению личности (ценностно-экспрессивная функция), выражаются в стремлении личности привести в систему содержащиеся в них личностные смыслы знаний, норм, ценностей (познавательная функция).

В процессе формирования антитеррористического мышления должны использоваться технологии направленного формирования ценностно-смысловых установок, ориентированые на особенности развития смысловых ориентиров тех, кто знакомится с ее содержанием. При этом должны быть сформированы:

- операциональные ценностно-смысловые установки, которые проявляют свою регулятивную функцию в готовности к негативной оценке терроризма;

- целевые установки, которые реализуются в стремлении согласовывать выбор целей и присвоения содержания антитеррористической деятельности на личностном уровне;

- мотивационные установки, которые проявляются в устойчивой тенденции к образованию категориального аппарата и языка антитеррористического мышления, стремлении вести себя в соответствии с представлениями «Каким я хочу быть».

Смысловой установке должна предшествовать *перцептивная положительная установка* (по терминологии Панасюка А.Ю. – установка на восприятие), которая активизирует познавательный интерес того, кто

является субъектом воздействия, воздействует на его эмоциональную сферу («Интересно послушать, что он скажет», «Интересно посмотреть, что это такое»). Перцептивная установка не тождественна *смысловой установке*, которая актуализирует глубинное понимание «хочу докопаться до истины, хочу узнать, что за этим скрывается». Иначе говоря, установка человека на восприятие и усвоение предлагаемого содержания еще не означает, что у него есть смысловая установка (он может воспринимать ее отнюдь и не пристрастно). Но если у человека есть смысловая установка, то ей обязательно предшествует перцептивная.

Смысловая установка обеспечивает не просто понимание или усвоение изучаемого содержания, но, что самое основное, выводит знание на уровень личностного присвоения, личностного принятия.

Для реализации технологий направленного воздействия в реальной практике информационно-пропагандистской работы должны быть разработаны методы реализации технологий, которые станут реальным руководство для тех, кто не просто является носителем ценностей антитеррористического мышления (транслятор), но и ведет практическую работу по презентации этих ценностей в различных группах населения (респонденты).

Формирование ценностных установок антитеррористического мышления. В процессе убеждения установка того, кого убеждают (респондент) может проявляться в разных типах как по способу формирования, так и по особенностям влияния на специфику смыслового взаимодействия транслятора (того кто убеждает) и респондента. В процессе разработки технологии направленной трансляции ценностно-смысловых установок в информационно-пропагандисткой работе необходимо использовать механизмы смысловой интерференции (как усиление и увеличение смысловой тождественности между ними) как механизм расширения совместного ценностно-смыслового пространства (транслятора и

респондента), который определяется двумя взаимосвязанными, но и противоположно направленными процессами:

- персонализацией как процессом передачи ценностно-смысловых характеристик в процессе формирования собственного образа мира, как интенция экстериоризации концепции «Я» и самоотношения;

- персонификацией как процессом порождения личностных ценностей за счет проникновения к смыслам и ценностям транслятора при включении им ценностей антитеррористического мышления в собственный образ мира.

Для успешного развития ценностных ориентаций респондентов необходимо использовать технологии направленного воздействия на респондентов как систему, которая позволит убедить его в личностной ценности общественных норм и способов поведения, позиционируемых обществом как позитивные. Чтобы перевести убеждающую информацию, являющуюся пока ценностью лишь для транслятора, в личностно значимую и для респондента, последнему необходимо показать, что основанные на этой информации действия и поступки не только не будут противоречить его ценностным ориентациям, но и будут способствовать удовлетворению его определенных потребностей и соответствовать его ценностным ожиданиям.

При использовании методов убеждающих воздействий транслятор должен учитывать следующие *рекомендации*:

-респонденты в процессе формирования антитеррористического мышления решают и осваивают проблемы, имеющие для них определенную личностную ценность;

- транслятор чувствует себя по отношению к респондентам конгруэнтно, то есть проявляет себя таким человеком, какой он есть, выражая себя свободно;

- транслятор проявляет положительное отношение к респондентам, принимает их такими, каковы те есть;

- транслятор проявляет смысловую эмпатию к респонденту, что означает способность проникать в его внутренний мир, понимать его ценности и личностные смыслы, смотреть его глазами, оставаясь при этом самим собой;

- транслятор играет роль помощника и стимулятора личностно-центрированного респондента, создает психологический комфорт и свободу для него, установки антитеррористического мышления должны быть центрированы на его смысложизненных ценностях и перспективах развития.