КЛАССИФИКАЦИЯ ИНФОРМАЦИОННЫХ УГРОЗ СОВРЕМЕННОМУ ОБЩЕСТВУ

А.-А.В. Таран

Кафедра политических наук
Российский университет дружбы народов
ул. Миклухо-Маклая, 10а, Москва, Россия, 117198

В современном мире информация приобрела статус одного из основных ресурсов социального, политического и научно-технического развития. Однако процесс информатизации привел к появлению новых угроз: информационных войн, информационного терроризма, кибертерроризма. Все эти угрозы нацелены на психическое и интеллектуальное состояние общества. Информационный терроризм представляет собой распространение заведомо ложной информации с целью распространения в обществе непонимания и лишения людей возможности здраво мыслить.

Одна из основных проблем правоохранительных органов в борьбе с кибертерроризмом — определить подлинных виновных лиц и оценить степень угрозы и возможных последствий преступлений в информационной сфере. Автор приходит к выводу, что в современном мире отдельное государство неспособно в одиночку эффективно справляться с информационным и кибертерроризмом. Только эффективное международное сотрудничество способно решить эту проблему.

Ключевые слова: информационное общество, кибертерроризм, информационный терроризм, национальная безопасность.

В современном обществе первостепенное значение приобрела информация (сообщение о некотором положении дел, передаваемое людьми; величина уменьшаемой неопределенности в результате получения сообщения; управленческие сигналы в единстве их синтаксической, семантической характеристик; мера разнообразия в объектах и процессах и т.д.) [13]. Информация стала главным ресурсом социального, политического, экономического и научно-технического развития в мире. В жизнь плотно вошли термины: информационное общество (концепция постиндустриального общества; новая историческая фаза развития цивилизации, в которой главными продуктами производства являются информация и знания) [13], информационное поле, информационная политика [8. С. 125], информационная война. Информационно-психологическая война является наиболее ярким примером острого информационно-психологического конфликта, характеризующегося высокой степенью интенсивности, агрессивности и социальной опасности [8].

Информационное поле создается за счет быстрого распределения и передачи информации между людьми посредством средств связи, СМИ и, в особенности, сети Интернет. Благодаря развитию Интернета появляется, фактически, новая виртуальная среда обитания человека, среда, в которой оказывается не только человек, но и целые механизмы управления и влияния на человека [11]. Для информационного пространства общества характерны некоторые уникальные субъекты и сообщества, не имеющие прямых аналогов в иных пространствах. К таковым относятся:

— социальное виртуальное сообщество (ВСС);

— онлайновое сообщество;

— сетевой социум;

— виртуальная коалиция.

Мотивации пользователей Интернета — побуждения, вызывающие активность и определяющие направленность пользователей на работу в сетевом информационном пространстве. Можно говорить о следующих мотивациях: деловая, познавательная, сотрудничество, самореализация, игровая, коммуникативная.

В обозначенных условиях развития актуальность приобрели такие понятия, как *информационный терроризм* и *кибертерроризм*. Не только в обществе, но и в исследованиях специалистов эти понятия часто подменяют друг другом либо считают синонимами [4]. Однако, структурировав информацию по теме и выявив характеристики понятий, можно сделать вывод, что это разные термины.

Информационный терроризм — психоинтеллектуальная опасная диверсия, направленная против нормального состояния разума людей [19]. Информационный терроризм производится посылами ложной информации для создания у людей противоречивого представления, негативного возмущения и ошибочного понимания [2].

Такой вид терроризма — предельно опасное асоциальное явление. Ничто так сильно не влияет на людей, общество и государство, как источники правдивой или ложной информации. Учитывая особую разрушительную мощь и характер непредсказуемых последствий диверсионного влияния дезинформации, информационный терроризм является, пожалуй, самым сложным. В отсутствие достоверных знаний информационные террористы умышленно дезориентируют нормальное сознание, представление и понимание людей об окружающих обстоятельствах в поле реального восприятия действительности [18], вызывая тем самым реальные действия — акции протеста, дестабилизацию общества.

Таким образом, информационный терроризм — это форма негативного воздействия на личность, общество и государство всеми видами информации. Одной из его целей является ослабление и расшатывание устоявшегося общественного строя посредством спецслужб, СМИ, заявлений авторитетных людей.

Информационный терроризм применяется, как правило, в областях, где есть предпосылки к идейной или финансовой борьбе, например, политика, экономика, религия и т.п. [10].

Механизмы информационного террора:

— создание общественных организаций определенного толка;

— формирование общественного мнения посредством СМИ (пресса, телевидение, Интернет);

— распространение агитационных и информационных материалов.

Таким образом, информационный терроризм, по сути, не влечет за собой быстрого физического уничтожения людей, однако последствия такого вида терроризма могут быть куда более трагическими. Так как общество стало информационным, то чтобы навязать ему определенные линии поведения, необходимо начать управлять информацией, циркулирующей по информационным потокам общества. Этим и пользуются террористы [1]. Информационный терроризм, как директивное навязывание малой группой людей определенных линий поведения власти

и обществу, пока еще малозаметен, плюс ко всему необходимо подчеркнуть, что информационный терроризм достигает своей цели незаметно для общества. Однако у нового поколения терроризма есть существенный недостаток, выражающийся в том, что информация имеет свойство мутации, и общество меняется, но не всегда в том направлении, в котором планируют разработчики. Поэтому можно выделить два направления в этой деятельности: первое — это «безмотивный терроризм», а второе — целенаправленный терроризм, который требует постоянной коррекции внедряемой информации [3].

Информационный терроризм поражает три основных зоны:

а) бытовую, когда поражение несет локализованный личностный характер;

б) научную, когда разрушаются объективно-закономерные логические связи проверенных научных истин;

в) социально-политическую, когда на национально-государственном (всемирном) уровне обманывается все население человечества-социума-сообщества многочисленных народов-наций-цивилизаций [17].

Кибертерроризм можно определить как атаку на информационную систему. То есть кибертерроризм — это инструмент и составляющая для информационного терроризма в целом. Киберпреступность — это преступность в так называемом «виртуальном пространстве» [15].

Кибертерроризм ориентируется на использование различных форм и методов вывода из строя информационной инфраструктуры государства или на использование информационной инфраструктуры для создания обстановки, приводящей к катастрофическим последствиям для общества и государства.

Число пользователей Интернета в мире впервые превысило 1 млрд человек. Такие данные приведены в «Докладе об информационной экономике», составленном Конференцией ООН по торговле и развитию. Согласно документу, к началу 2006 года доступом в глобальную сеть обладали 1 млрд 20 млн 610 тыс. человек. По сравнению с предыдущим годом этот показатель вырос на 19,5% [16].

В первую тройку стран по числу интернет-пользователей вошли США — около 200 млн, Китай — 111 млн и Япония — 85,29 млн человек.

В России число пользователей «всемирной паутины» на конец 2005 года составляло 21,8 млн человек, увеличившись за год на 17,8%. По этому показателю Россия находится на 11-м месте в мире и на первом среди стран Восточной Европы и СНГ. Следом за ней идут Украина (4,5 млн человек) и Белоруссия (3,39 млн) [16].

По заявлениям некоторых иностранных экспертов, отключение всех компьютерных систем приведет к разорению 20% средних компаний в течение нескольких часов, 48% потерпят крах в течение нескольких суток. Около 33% банков будут разорены спустя несколько часов после такой катастрофы, а 50% из них разорятся спустя несколько суток (см.: [5]).

В Доктрине информационной безопасности Российской Федерации подчеркивается, что информационная сфера, являясь системообразующим фактором жизни общества, активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности Российской Федерации [6. С. 4].

Помимо этого, информационная сфера сейчас рассматривается как новый экономический, культурный и политический капитал, особенно подверженный новым формам преступности. Стремительное развитие телекоммуникаций и глобальных компьютерных сетей создало условия, облегчающие совершение преступлений в сфере компьютерной информации [7].

Использование сравнительно недорогих персональных и домашних компьютеров (в России осенью 2002 г. было примерно 8,7 млн пользователей, зимой 2004—2005 гг. — уже 17,6 млн (16% населения), всеобщая доступность в сети Интернет информации, ранее являвшейся достоянием лишь узкого круга специалистов, в том числе данных об информационной безопасности и методах «взлома» компьютеров, расширили возможности для совершения компьютерных преступлений [14. С. 4].

В течение последних лет международное сообщество проявляет значительный интерес к проблеме борьбы с киберпреступлениями. В связи с этим были разработаны несколько международно-правовых документов [17].

В России с каждым годом растет количество преступлений, совершаемых в сфере компьютерной информации (Глава 28 Уголовного кодекса РФ предусматривает ответственность за данный вид деяний. Впервые введена в действие с 01.01.1997). Так, по данным ГИЦ МВД РФ, в 2002 г. правоохранительные органы по ст. 272—274 УК РФ зарегистрировали 4050 преступлений. Для сравнения: по данным того же ГИЦ МВД, по ст. 272—274 УК РФ в 2000 г. было возбуждено 584 уголовных дела, в 2001 г. выявлено 3720 преступлений, в 2003 году уже 10 375. Это более чем в 2,5 раза превышает уровень 2002 года [20]. По оценкам зарубежных специалистов, ущерб, который деструктивная деятельность в информационной сфере нанесла мировой экономике, связывают с возрастающей активностью «хакеров». Потери от сетевых атак: 2000 год — 24 млрд долларов США, 2001-й — 34 млрд долларов США, 2002-й — 49 млрд долларов США, 2003 год — более 60 млрд долларов США [12].

Еще в 2001 году Межведомственной комиссией Совета Безопасности Российской Федерации по информационной безопасности одобрены «Основные направления нормативного правового обеспечения информационной безопасности Российской Федерации» (Решение № 5.4 от 27.11.01), согласно которым в число первоочередных мер по совершенствованию нормативного правового обеспечения информационной безопасности включена разработка следующих законопроектов: «О персональных данных», «О праве на информацию», «О коммерческой тайне», «О неприкосновенности частной жизни, о личной и семейной тайне», «О защите нравственности», «О служебной тайне», «О национальной безопасности» [9].

Существует несколько способов использования Интернета для содействия террористическим группам:

— сбор информации о целях (например, трубопровод, ЛЭП);

— сбор средств (например, игра на бирже);

— возможность объединить людей (в том числе из разных государств);

— дискредитация лиц, групп лиц и государственного режима в целом;

— психологический террор, акции запугивания населения;

— коммуникация между террористами.

Одной из главных проблем в борьбе с преступностью, в том числе с кибертерроризмом, в информационном обществе является трудность в идентификации виновного лица и оценке масштабов последствий преступного деяния. Поскольку данные информационных систем и сетей не всегда являются статическими, традиционные процедуры сбора данных, относящиеся к электросвязи, такие как сбор данных в режиме реального времени и перехват контента, должны быть адаптированы для целей обеспечения сбора электронных данных. Некоторые из этих мер изложены в Рекомендации Совета Европы № R(95)13 по проблемам уголовно-процессуального права, связанным с информационными технологиями.

Таким образом, можно говорить о том, что ни одно отдельное государство не способно эффективно противостоять информационному терроризму и кибертерроризму. Возможно только эффективное международное сотрудничество.

ЛИТЕРАТУРА

[1] *Алексеева И.Ю.* Информационные вызовы национальной и международной безопасности. — М.: ПИР-Центр, 2001.

[2] *Антюхов В.И., Жуков Ю.И., Кадулин В.Е., Примакин А.И.* Информационный терроризм: прошлое, настоящее и будущее. — СПб.: МВД России, 2000.

[3] *Бианки В.А., Серавин А.И.* Практика и психология регионального партстроительства. — СПб., 2006.

[4] *Газизов Р.Р.* Информационный терроризм. Материалы международной научно-практической конференции 16—17 октября 2003 года. Часть I. — Уфа: РИО БашГУ, 2003.

[5] *Гриняев С.Н.* Информационный терроризм: предпосылки и возможные последствия // Журнал теории и практики Евразийства.

[6] Доктрина информационной безопасности Российской Федерации // Российская газета. — 28 сентября 2000 г.

[7] Компьютерная преступность и кибертерроризм: Сборник научных статей / Под ред. В.А. Голубева, Н.Н. Ахтырской. — Запорожье: Центр исследования компьютерной преступности, 2004. — Вып. 1.

[8] *Манойло А.В.* Государственная информационная политика в особых условиях. — М., 2003.

[9] *Полякова Т.А.* Проблемы правового обеспечения доступа к информации // Бизнес и безопасность в России. — 2004. — № 38.

[10] *Почепцов Г.Г.* Информационные войны. — М., 2000.

[11] *Почепцов Г.Г.* Информационно-психологическая война. — М., 2000.

[12] *Родионов С.Н., Устюгов С.В.* Аппарат Совета Безопасности Российской Федерации // Бизнес и безопасность в России. — 2004. — № 38.

[13] Российский гуманитарный энциклопедический словарь. — М.: ВЛАДОС, 2002.

[14] Фонд «Общественное мнение» // Опросы «Интернет в России» 2004—2005. — Вып. № 10.

[15] *Голубев В.* «Кибертерроризм» — миф или реальность?» // http://www.crime-research.org

[16] Доклад об информационной экономике // http://www.prime-tass.ru

[17] Европейская Конвенция по борьбе с киберпреступностью от 9 ноября 2001 года // http://www.coe.int

[18] *Кулибаба А.Н.* Информационный терроризм. — http://www.inauka.ru

[19] Материалы конференции 6 апреля 2005 г. на третьем международном конгрессе по борьбе с киберпреступностью в Лондоне // РИА «Новости» // www.rian.ru

[20] Статистические данные МВД РФ за 2003 год // www.mvdinform.ru
[21] Статистические данные МВД РФ за период с января по сентябрь 2005 года // www.mvdinform.ru

CLASSIFICATION OF INFORMATION THREATS TO MODERN SOCIETY

A.-A.V. Taran

The Department of Political Science
Russian People's Friendship University
Miklucho-Maklaya str., 10a, Moscow, Russia, 117198

Information became the main resource of social, political, economic and scientific-technical development in the world. Besides the development of information new threats to the society have appeared: information wars, information terrorism, cyber terrorism. All these phenomena are psycho intellectual dangerous diversion. Information terrorism is characterized by the spreading of the false information in order to breed by people misconception and misunderstanding.

One of the main problems in the struggle against criminality, including against cyber terrorism in the information society is that it is difficult to find the guilty person and estimate the scale of aftermaths of a crime. Thus, one can say that any state is not able to withstand by itself efficiently information terrorism and cyber terrorism, only efficient international cooperation is possible.

Key words: information society, cyber terrorism, information terrorism, national security.