

**ТЕРРОРИСТИЧЕСКАЯ
ДЕЯТЕЛЬНОСТЬ В УСЛОВИЯХ НОВЫХ
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ_____**

Информационно-коммуникационные технологии (ИКТ) давно признаны эффективным инструментом содействия делу мира, безопасности и стабильности, укрепления демократии, социальной сплоченности граждан, надлежащего управления и верховенства права на национальном, региональном и международном уровнях. ИКТ также используются для содействия экономическому развитию общества, повышению эффективности социальной политики, развитию политической культуры граждан.

Негативный момент развития ИКТ – возможность их использования для нарушения международного мира и безопасности, совершения преступлений, подготовки и осуществления террористических актов, распространения террористической идеологии и практики разрешения противоречий общественного развития.

Украина, «інтегруючись у європейський процес, не може бути осторонь проблем сучасних міждержавних відносин. Тероризм – одна з них, отже, своєрідним каталізатором розвитку цієї проблеми в Україні може стати її відкрита зовнішньополітична діяльність».¹⁾

Как следует из определения терроризма, данного в Законе Украины «О борьбе с терроризмом», «Терроризм – общественно опасная деятельность, состоящая в сознательном, целенаправленном применении насилия путем захвата заложников, поджогов, убийств, пыток, запугивания населения и органов власти или совершения иных посягательств на жизнь или здоровье ни в чем ни повинных людей либо угрозы совершения преступных действий с целью достижения преступных целей».²⁾

Сегодня наряду с привычными типами террористических группировок действуют организации нового типа, со значительно менее выраженной националистической или идеологической идентичностью.³⁾

Терроризм нового типа получил название «терроризм в прямом эфире» или «информационный терроризм». Его цель – не только уничтожение представителей политической элиты, но и дезорганизация и запугивание всего общества. Информационный терроризм – это форма негативного влияния на личность, общество и государство всеми видами информации. Его цель – ослабление конституционного строя.⁴⁾

Все чаще информационный терроризм направляется на простых граждан, а не, как было раньше, на соответствующие руководящие системы.⁵⁾ А уже простые граждане выражают свое недовольство властью, не способной их защитить от проявлений терроризма.

По имеющимся данным, в настоящее время в 70 странах насчитывается около тысячи групп и организаций, использующих в своей деятельности методы террора.⁶⁾ Бурный научно-технический прогресс вооружил террористические организации новыми технологиями в ядерной, биологической, химической, информационной сфере, которые, по их замыслу, позволят осуществить человеконенавистнические цели.

Среди исследователей проблем терроризма нет единодушия относительно трактовки сущности терроризма, в частности, международного. Так, одни исследователи делают акцент на средствах, способах деяния – осуждают преступные и антигуманные. Для других – главным оказывается мотивация, побудительные причины противозаконного деяния.⁷⁾ Как считает Ф. Ильясов, «терроризм – это убийство, запугивание мирного населения, оказание психологического давления, используемые ради достижения экономических и социальных целей».⁸⁾

Исключительно большую опасность в современных условиях представляет технологический терроризм, включающий в себя

информационный терроризм (кибертерроризм, биотерроризм, «ядерный терроризм») и возможное использование расщепляющихся ядерных материалов и химического оружия.

Информационно-коммуникационные технологии приобретают свойства оружия, поражающие свойства которого будут возрастать по мере дальнейшего совершенствования ИКТ, расширения их повсеместного использования, развития информационной инфраструктур общества и государства, информатизации вооружения и военной техники.⁹⁾

Современные информационные технологии интенсивно используются для подготовки, планирования и осуществления террористических актов, вербовки новых членов террористические организации, пропаганды экстремистской, в том числе, террористической идеологии.¹⁰⁾

Новой тенденцией в эволюции терроризма стал кибертерроризм. Его политическая цель – нагнетание общественной напряженности, страха, дестабилизация обстановки, дискредитация официальной власти. Фактической целью его атак выступают компьютерные системы управления критической инфраструктурой, то есть транспортом, атомными электростанциями, водоснабжением и энергетикой.¹¹⁾

Выработкой механизмов решения вопросов киберпреступности занимаются такие организации, как Форум по управлению Интернетом, образованный по итогам Всемирной встречи на высшем уровне по вопросам информационного общества, Международный союз электросвязи, ряд негосударственных организаций, экспертное сообщество.

Специфика информационного терроризма не в физическом уничтожении людей, ликвидации материальных ценностей, разрушении жизненно важных объектов, а в нарушении работы информационно-коммуникативных сетей. Сети министерства обороны США выдерживают шесть миллионов хакерских атак в день.¹²⁾

Система Internet, связавшая компьютерные сети по всей планете, изменила правила, касающиеся современного оружия. Анонимность, обеспечиваемая InternetoM, позволяет террористу стать невидимым, как следствие, практически неуязвимым и ничем (в первую очередь жизнью) не рискующим при проведении преступной акции.¹³⁾

Специалисты полагают, что в мире высоких технологий уже сейчас возможны неординарные террористические акты. Например, овладев компьютером, который управляет самолетом, можно диктовать свою волю экипажу и наземным службам, даже не совершая вооруженного захвата.¹⁴⁾

Необходимо совершенствовать информационную политику Украины. Используя опыт западных стран, следует не только учитывать негативные информационные влияния и воздействия (что, безусловно, важно), но, в первую очередь, разработать стратегию и тактику информационной войны.

ДЖЕРЕЛА ТА ЛІТЕРАТУРА

- 1) Руденко М. М. Інформаційний чинник політики США і Росії в питанні міжнародного тероризму: Автореф. дис канд. політ. наук: спец. 23.00.04 – політичні проблеми міжнародних систем та глобального розвитку / М. М. Руденко. – К., 2004. – С. 15.
- 2) Закон України «Про боротьбу з тероризмом» № 638-4 від 20. 03. 2000 р. <http://dspace.onu.edu.ua:8080/bitstream/123456789/6417/1/48-50.pdf>
- 3) Недбай В. В. Социально-политические последствия развития информационного общества: Дис. канд. полит. наук : спец. 23.00.02 – политические институты и процессы / В. В. Недбай. – Одесса, 2004. – С. 71-72.
- 4) Назаренко С. І. ЗМІ – неупереджений свідок чи мимовільний учасник терористичної діяльності / С. І. Назаренко // Сучасна українська

- політика. Політики і політологи про неї. – Вип. 19. – К., 2010. – С. 265, 267.
- 5) Там само.
 - 6) Набиев В. Государственная политика в области международного сотрудничества по борьбе с терроризмом / В. Набиев // Власть. – 2007. – № 8. – С. 23-30.
 - 7) Назаренко С. І. – Указана праця. – С. 265.
 - 8) Ильясов Ф. Н. Терроризм – от социальных оснований до поведения жертв / Ф. Н. Ильясов // Социологические исследования. – 2007. – № 6. – С. 82.
 - 9) Тезисы выступления директора Института проблем информационной безопасности МГУ имени М. В. Ломоносова В. П. Шерстюка [Электронный ресурс]. – Режим доступа: <http://www.iisi.msu.ru/news/news35/>
 - 10) Гриняев С. Россия в глобальном информационном обществе: угрозы, риски и возможные пути их нейтрализации / С. Гриняев [Электронный ресурс]. – Режим доступа: <http://www.fondiv.ru/articles/3/335/>.
 - 11) Додин И. С. Информационно-коммуникационные технологии в системе государственного управления регионом : Автореф. дис канд. полит, наук : спец. 23.00.02. – политические институты, этнополитическая конфликтология, национальные и политические процессы и технологии (по политическим наукам) / И. С. Додин. – Саратов, 2007. – С. 13.
 - 12) Сети Пентагона атакуют шесть миллионов раз в день [Электронный ресурс]. – Режим доступа: <http://www.itsec.ru/newstext.php7newsid=67603>
 - 13) Величко М. Ю. Информационная безопасность в деятельности органов внутренних дел: теоретико-правовой аспект : Автореф. дис. ... канд.

юрид. наук : спец. 12.00.01 – теория и история права и государства;
история учений о праве и государстве / М. Ю. Величко. – Казань, 2007. –
С. 18.

- ¹⁴⁾ Томчак Е. В. Из истории компьютерного терроризма /Е. В. Томчак
//Новая и новейшая история. – 2007. – № 1. – С. 42.