

РЕЗЮМЕ

Тема исследования: Кибертерроризм как угроза национальной безопасности Российской Федерации.

Автор: Михаил Клименский.

Научный руководитель: Соловьева Е.А., старший преподаватель, кандидат политических наук.

Организация: Институт международных отношений; Кафедра международных отношений, мировой экономики и международного права; Пятигорский государственный лингвистический университет.

Актуальность темы исследования определяется существенным ростом коммуникативности в современной социально-политической среде, который активизировал использование информации и информационных потоков как в благоприятных, так и в деструктивно-ориентированных целях. В результате данных тенденций возникли такие новые явления, как информационные войны, использование СМИ в экстремистских и террористических целях, кибертерроризм. Данные процессы, являясь новым компонентом в системе угроз национальной и международной безопасности, требуют изучения и политологической концептуализации.

Цель исследования состоит в том, чтобы изучить кибертерроризм как новый элемент в структуре угроз национальной безопасности Российской Федерации и пути его нейтрализации.

Задачи исследования:

- изучить концептуальные подходы к определению понятия кибертерроризм в контексте политической науки;
- исследовать кибертерроризм как социально-политическое явление, представляющее угрозу национальной безопасности;
- проанализировать российский и международный опыт противодействия кибертерроризму;
- Разработать рекомендации по совершенствованию государственной политики РФ по противодействию кибертерроризму.

Научная новизна исследования: В ходе исследования были систематизированы концептуальные подходы к определению понятия «кибертерроризм». Были определены факторы, порождающие кибертерроризм в Российской Федерации, отличительные признаки и тенденции его функционирования на современном этапе. Был проведен компаративный анализ международного опыта государств в сфере противодействия кибертерроризму. Также были предложены основные направления повышения эффективности политики противодействия кибертерроризму в России.

Структура работы: введение, две главы, включающие по 2 параграфа каждая, заключение, библиографический список использованной литературы из 105 источников, в том числе 22 из них – на иностранных языках, и 9 приложений. Общий объем работы составляет 86 страниц машинописного текста.

Резюме: В современном мире невозможно представить нашу жизнь без компьютерных систем, глобальной сети, через которую осуществляется коммуникация, обмен и хранение информации, а также управление и контроль банковских систем, инфраструктуры отраслей промышленности и даже боевых систем и военных объектов.

В этой связи можно сделать вывод, что кибербезопасность, являясь составной частью информационной безопасности, становится одним из ключевых аспектов национальной безопасности государства.

Политический, социальный и экономический факторы комплексно способствуют зарождению кибертерроризма в РФ. Его фундаментальными признаками выступают – публичный характер, удаленность от места осуществления террористического акта, анонимность. В качестве текущих тенденций, характеризующих развитие кибертеррористической угрозы в РФ на современном этапе, являются политизация кибертерроризма, рост уровня формируемой им угрозы, а также рост технологической оснащенности субъектов исполнителей.

Учитывая факторы, порождающие кибертерроризм, предупреждение кибертеррактов представляет собой сложную задачу. Следовательно, политические, социальные, экономические, исторические, психологические причины должны быть объектом постоянного внимания и профилактического вмешательства со стороны государства и гражданского общества.

Для успешного противодействия кибертерроризму необходимо принятие всеобъемлющих законов об электронной безопасности, в соответствии с действующими международными стандартами, организация эффективного сотрудничества с иностранными государствами, их правоохранительными органами и спецслужбами, а также с международными организациями, и создание национальных подразделений по борьбе с киберпреступностью и международного контактного пункта по оказанию помощи для реагирования на транснациональные компьютерные инциденты.