Док.GA40/LC40/REC129/12/r

РЕКОМЕНДАЦИЯ 129/2012[1]

«О роли парламентов в укреплении информационной (кибер) безопасности в государствах-членах ЧЭС»

1. Парламентская Ассамблея Организации Черноморского Экономического Сотрудничества (ПАЧЭС) подчеркивает, что кибербезопасность является одним из приоритетных вопросов современности. Этот вопрос продолжает приобретать значение в соответствии с постоянным ростом зависимости от информационных технологий почти в каждой сфере жизни. Риск, сопутствующий расширяющемуся межсетевому взаимодействию, заключается в том, что информационные системы и сети становятся открытыми для возрастающего количества угроз и видов уязвимости, влекущих за собой проблемы безопасности для всех пользователей.

2. ПАЧЭС осознает, что киберпространство оказывает существенное влияние на практически каждого человека и каждую область жизни. Новые информационные технологии сжимают пространство и время, предлагая молниеносный доступ к огромному количеству знаний и обеспечивая мгновенный обмен информацией. Масштаб взаимосвязи наряду с динамизмом технологического развития влекут за собой сопутствующие проблемы кибербезопасности.

3. ПАЧЭС понимает, что широко распространенный доступ к легко регулируемой цифровой инфраструктуре имеет позитивное значение для общего развития и прогресса, однако кибератаки обладают потенциалом трансформирования уязвимости в разрушительные силы с серьёзными последствиями. Кибербезопасность является многогранным феноменом с многослойными последствиями.

4. ПАЧЭС признает, что для противостояния кибератакам необходимы хорошо отлаженные мощности, способные устранить уязвимые места. Необходима расширенная инфраструктура кибербезопасности для того, чтобы

---

[1] *Докладчик*: г-н Сергей Подгорный, Председатель Комитета - Украина

Дискуссия Ассамблеи 27 ноября 2012 г. (см. Док.: GA40/LC40/REP/12/r, доклад Комитета по правовым и политическим вопросам *«Роль парламента в укреплении информационной (кибер) безопасности в государствах-членах ЧЭС»*, обсужденный в Афинах 17 октября 2012 г., докладчик: г-н Михаил Емельянов, заместитель Председателя Комитета, Россия).

Текст одобрен на Сороковой Генеральной Ассамблее в Баку 27 ноября 2012 г.)

индивидуальные граждане и мировое сообщество смогли реализовать в полной мере потенциал революционных информационных технологий.

5. Ассамблея призывает национальные парламенты принять необходимые меры безопасности в киберпространстве. Эти меры должны осуществляться своевременно и в соответствии с ценностями, признаваемыми демократическим обществом: свободой обмена мнениями, свободными потоками информации, конфиденциальностью информации и сообщений, и соответствующей защитой личной информации.

6. ПАЧЭС признает, что государства-члены ЧЭС стоят перед двойственным вызовом поддержания среды, способствующей развитию инноваций и технологий, обеспечивая при этом надёжность, безопасность и права неприкосновенности частной жизни. Основной обязанностью правительств является устранение уязвимых мест в киберпространстве и обеспечение использования глобальным сообществом потенциала революционных информационных технологий в полной мере. Маловероятно, что без существенного прогресса в обеспечении безопасности этих систем или значительных изменений в их создании и эксплуатации государства-члены смогут защитить себя от возрастающей угрозы киберпреступности и вторжений.

7. ПАЧЭС положительно оценивает деятельность Рабочей группы ЧЭС по науке и технологии, в частности, подготовку важных документов в сфере технологического развития. Она выражает надежду, что Рабочая группа будет и дальше развивать инициативу создания взаимоприемлемых условий функционирования сети международных центров по предупреждению и противостоянию кибератакам с целью выработки надежных механизмов кибербезопасности.

8. ПАЧЭС считает, что вопросы кибербезопасности имеют транснациональный характер в силу международной архитектуры и глобального распространения киберпространства, что делает эффективное международное сотрудничество необходимым условием для принятия мер по кибербезопасности. Она одобряет возрастающее международное сотрудничество в решении вопросов противостояния вызовам киберпространству, и решительно поддерживает меры по выработке политики, направленной против сбоя в работе информационных систем и предусматривающей ответные действия на угрозы кибербезопасности, предпринятые Советом Европы, Организацией экономического сотрудничества и развития (ОЭСР), Организацией по безопасности и сотрудничеству в Европе (ОБСЕ), Организацией Североатлантического договора (НАТО), Организацией объединенных наций (ООН) и Европейским Союзом (ЕС).

9. ПАЧЭС подчеркивает, что, несмотря на возрастающее понимание значения кибербезопасности и мер, предпринятых для укрепления безопасности, киберриски продолжают представлять угрозу для информационных сетей и систем. К сожалению, ни одна отдельная стратегия не может полностью устранить уязвимые места и связанные с этим риски в киберпространстве. Ассамблея понимает, что защита киберпространства представляет собой постоянно развивающийся процесс, поскольку появляются новые технологии и определяются новые уязвимые места.

10. **В связи с этим, Ассамблея рекомендует** парламентам и правительствам государств-членов ЧЭС:

i. *заручиться* поддержкой национальных парламентов в укреплении межпарламентского регионального и международного сотрудничества по укреплению национальных и международных правовых рамок, направленных на сдерживание и предупреждение киберпреступности;

ii. *способствовать* предотвращению угроз криминального и террористического характера, а также обеспечивать соблюдение норм международного права, включая принципы уважения суверенитета и невмешательства во внутренние дела других государств;

iii. *способствовать* взаимному оказанию правовой поддержки и сотрудничеству между судебными органами путем подписания, ратификации и осуществления, при необходимости, резолюций ООН, касающихся кибербезопасности: Резолюции 56/121 «О борьбе с использованием информационной технологии в преступных целях», Резолюции 57/239 «О создании глобальной культуры кибербезопасности»; Резолюции 64/422 «О глобализации и взаимозависимости; наука и технология на благо развития» резолюции 64/386 «О событиях в области информации и телекоммуникаций в контексте международной безопасности»;

iv. *обеспечивать* эффективное использование всех механизмов эффективного национального и международного сотрудничества по укреплению кибербезопасности путем подписания и осуществления, при необходимости, двусторонних и многосторонних соглашений;

v. *оказывать поддержку* более широкому прямому сотрудничеству между судебными и правоохранительными органами в сфере кибербезопасности;

vi. *приводить с исполнение и вносить поправки* в соответствующие законодательные меры согласно международным нормам и стандартам в сфере кибербезопасности;

vii. *укреплять* региональное сотрудничество с помощью приемлемых международных правовых инструментов по вопросам кибербезопасности и их гармонизации с национальным уголовным кодексом;

viii. *осуществлять* необходимые меры по укреплению, где это необходимо, правоохранительных органов и способствовать эффективной работе и взаимодействию между национальными структурами, занимающимися укреплением кибербезопасности;

ix. *установить* приоритетность финансирования науки, технологии и инноваций с целью продвижения, стимулирования и совершенствования исследований, отвечающих национальным приоритетам и стратегическим задачам в сфере кибербезопасности;

x. *максимально* использовать имеющиеся правовые механизмы для всеобъемлющей национальной программы повышения осведомленности в сфере кибербезопасности с целью пропаганды преимуществ технологического развития и оказания ему поддержки, сводя при этом к минимуму и смягчая ущерб от возможных кибератак;

xi. *способствовать* созданию многоуровневых систем безопасности, защищающих источники информации и предупреждающих несанкционированный доступ к информации;

xii. *одобрять* инициативы по созданию взаимоприемлемых условий функционирования сети международных центров по предупреждению и отражению кибератак с целью выработки надёжных механизмов для безопасного доступа и обмена информацией;

xiii. *направлять усилия* на расширенное взаимодействие и координирование действий правоохранительных органов, служб разведки и судебных органов с целью соответствующей подготовки для борьбы с кибератаками и вторжениями;

xiv. *содействовать* проведению курсов профессиональной подготовки для сотрудников правоохранительных и судебных органов по вопросам киберпреступности и негативных последствий подобных действий для индивидуума и общества;

xv. *улучшать* обмен информацией о национальном законодательстве в сфере предупреждения кибертерроризма и борьбы с ним и другими взаимосвязанными киберпреступлениями, а также осуществлять мониторинг его исполнения;

xvi. *обеспечивать* координацию и сотрудничество специализированных национальных агентств при соответствующих министерствах с целью включения вопроса безопасности как необходимого элемента планирования, дизайна, функционирования и использования информационных систем и сетей.

11. **Ассамблея предлагает** Совету министров иностранных дел ЧЭС рассмотреть настоящую рекомендацию