ПАРЛАМЕНТСКАЯ АССАМБЛЕЯ ЧЕРНОМОРСКОГО ЭКОНОМИЧЕСКОГО СОТРУДНИЧЕСТВА
ПАЧЭС

МЕЖДУНАРОДНЫЙ СЕКРЕТАРИАТ

Док.GA51/LC51/REC162/18/r

РЕКОМЕНДАЦИЯ 162/2018[1]

«Укрепление сотрудничества в области кибербезопасности в государствах-членах ЧЭС»

1. Парламентская Ассамблея Организации Черноморского Экономического Сотрудничества (ПАЧЭС) подчеркивает, что кибербезопасность является одним из главных приоритетов современности. Вызовы XXI столетия требуют развития новых информационно-коммуникационных технологий, которые открывают широкие возможности для человеческой деятельности. Сложные, многослойные информационные потоки способствуют развитию и укреплению человеческого потенциала и нацелены на достижение высокого уровня развития жизни и блага миллионов людей во всем мире.

2. ПАЧЭС отмечает, что в современном мире киберпространство касается практически всех и каждого, кто является частью глобальной информационной системы. Глобально взаимосвязанная цифровая информация и инфраструктура связи составляют основу практически каждой сферы современной деятельности и обеспечивает важную поддержку экономике, общественной инфраструктуре, общественной и национальной безопасности. Масштаб взаимосвязи наряду с динамизмом технологического развития влекут за собой сопутствующие проблемы кибербезопасности.

3. ПАЧЭС напоминает о своей Рекомендации 129/2012 «О роли парламентов в укреплении информационной (кибер) безопасности в государствах-членах ЧЭС», в которой подчеркивается важность разделения ответственности с целью противостоять потенциальным угрозам и максимально использовать преимущества и возможности, обеспечиваемые информационно-

---

[1] Дискуссия Ассамблеи 20 июня 2018 г. (см. Док.: GA51/LC51/REP/18/r, Доклад Комитета по правовым и политическим вопросам *«Укрепление сотрудничества в области кибербезопасности в государствах-членах ЧЭС»*, обсужденный в Тиране 19 июня 2018 г., докладчик: г-н Эльдар Гулиев, заместитель Председателя Комитета, Азербайджан).

Текст одобрен на Пятьдесят первой Генеральной Ассамблее в Тиране 20 июня 2018 г.)

коммуникационными технологиями в безопасной среде, как важного элемента достижения устойчивого развития. В документе также подчеркивается, что парламенты должны определять приоритеты финансирования в науку, технологию и инновации для стимулирования и расширения исследований с тем, чтобы адекватно реагировать на эти угрозы и вовремя справляться с ними.

4. ПАЧЭС понимает, что слаженно функционирующее киберпространство способствует развитию и прогрессу, однако, кибератаки могут трансформировать уязвимость компьютерной системы в разрушительную силу и привести к серьезным последствиям. Обеспечение надежности и безопасности киберпространства представляет собой сложную стратегическую задачу, требующую скоординированных и целенаправленных действий со стороны всего общества – государства, частного сектора и населения.

5. Ассамблея призывает к своевременному осуществлению необходимых мер на всех уровнях. Политика в области кибербезопасности должна включать стратегию и новейшие стандарты безопасности операций в киберпространстве, а также охватывать полный спектр действий по снижению угроз и уязвимости, повышению безопасности информации.

6. ПАЧЭС подчеркивает, что государства-члены ЧЭС проявляют все больше активности в вопросах обеспечения кибербезопасности и предпринимают всеобъемлющие меры по борьбе с киберугрозами, поддерживая среду, способствующую технологическому развитию, укрепляя при этом надежность и безопасность сетей. Они запускают широкомасштабные программы и инициативы для усиления кибербезопасности в ответ на вызовы, связанные с защитой соответствующих инициатив, в том числе в научно-исследовательской сфере.

7. ПАЧЭС приветствует деятельность Рабочей группы ЧЭС по науке и технологии, в частности, подготовку важных документов в сфере технологического развития в рамках текущего Плана действий. Ассамблея выражает надежду, что Рабочая группа будет развивать свою деятельность с целью внесения вклада в разработку механизмов развития и укрепления кибербезопасности.

8. ПАЧЭС считает, что на современные вызовы кибербезопасности можно реагировать в рамках международного сотрудничества и принятия скоординированных мер. Она поддерживает меры по выработке политики, направленной на угрозы кибербезопасности, предпринятые различными международными организациями.

9. ПАЧЭС отмечает важность национальных программ кибербезопасности для защиты граждан и национальной инфраструктуры от кибератак. Также необходимо достигнуть единства в вопросах кибербезопасности и объединить ресурсы по выявлению слабых мест и противодействию все большему спектру киберугроз.

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

i. *поддержать* создание более надежной, устойчивой и безопасной цифровой инфраструктуры;

ii. *принимать меры* по усилению межпарламентского сотрудничества по укреплению национальных и международных правовых рамок, направленных на сдерживание и предупреждение киберпреступности;

iii. *укреплять* региональное сотрудничество с помощью приемлемых международных правовых инструментов по вопросам кибербезопасности и их гармонизации с национальными уголовными кодексами;

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

v. *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;

vi. *установить* в режиме реального времени систему наблюдения, мониторинга и раннего предупреждения об атаках, а также инструментов реагирования на киберинциденты;

vii. *совершенствовать* стратегии кибербезопасности с целью обеспечения превентивного поиска и анализа вредоносных кодов в киберпространстве с высокой точностью, уменьшая вероятность допустить ошибку;

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

ix. *максимально* использовать имеющиеся правовые механизмы для успешного применения национальных программ повышения осведомленности в сфере кибербезопасности;

x. *проводить* комплексные меры по выявлению слабых мест ключевых ресурсов и важной инфраструктуры, постоянно оценивая потенциальные риски;

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

xii. *создать необходимые условия* для проведения целенаправленных совместных исследований в области обеспечения кибербезопасности с учетом краткосрочных, промежуточных и долгосрочных приоритетов;

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

xiv. *содействовать* сотрудничеству общественных институтов и частного сектора, уделяя больше внимания решению глобальных проблем кибербезопасности;

xv. *одобрять* инициативы по созданию необходимых условий функционирования сети международных центров по предупреждению

кибератак с целью выработки надежных механизмов для безопасного доступа и обмена информацией;

xvi. *содействовать* повышению профессиональной подготовки сотрудников правоохранительных и судебных органов по вопросам киберпреступности и негативных последствий подобных действий;

xvii. *обеспечивать* координацию и сотрудничество специализированных национальных агентств при соответствующих министерствах с целью включения вопроса кибербезопасности как необходимого элемента планирования, функционирования и использования информационных систем;

xviii. *интенсифицировать* обмен информацией о национальных законодательствах в сфере предупреждения кибертерроризма и борьбы с ним и другими взаимосвязанными киберпреступлениями, а также осуществлять мониторинг его исполнения;

xix. *способствовать* созданию онлайн платформы между организациями по кибербезопасности стран-членов ЧЭС на нескольких языках с целью осуществления обмена оперативной информацией о киберугрозах и киберинцидентах;

xx. *поддержать предложение* по проведению недели кибербезопасности в странах-членах ЧЭС по актуальным вопросам безопасного использования социальных сетей и защиты личной информации;

xxi. *активизировать* двустороннее и многостороннее сотрудничество для наращивания потенциала и повышения уровня информированности в области кибербезопасности;

xxii. *организовать* совместные конференции и семинары по новым киберугрозам и обеспечению кибербезопасности.

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