Док.: GA40/LC40/REP/12/r

СОРОКОВОЕ ЗАСЕДАНИЕ КОМИТЕТА ПО ПРАВОВЫМ И ПОЛИТИЧЕСКИМ ВОПРОСАМ

ДОКЛАД *

РОЛЬ ПАРЛАМЕНТОВ В УКРЕПЛЕНИИ ИНФОРМАЦИОННОЙ (КИБЕР) БЕЗОПАСНОСТИ В ГОСУДАРСТВАХ-ЧЛЕНАХ ЧЭС

Докладчик: г-н Михаил Емельянов, заместитель Председателя Комитета, Россия

* *Текст рассмотрен на Сороковом заседании Комитета по правовым и политическим вопросам в Афинах 17 октября 2012 г. и утвержден на Сороковой Генеральной Ассамблее в Баку 27 ноября 2012 г.*

I. ВСТУПЛЕНИЕ

В контексте глобального роста влияния информационных технологий безопасность этой отрасли становится главным вызовом для глобального сообщества, каждого отдельно взятого государства и человека. Новые информационно-коммуникационные технологии открывают совершенно новые возможности. Многослойные информационные потоки способствуют укреплению потенциала и нацелены на более высокий уровень развития на благо миллионов людей во всем мире. Из года в год возрастает зависимость от информационных технологий практически в любой сфере жизни, а вместе с тем, проблемы, связанные с киберпространством, приобретают всё более глобальный характер. Следовательно, риски, связанные с киберпространством, относятся к числу наиболее серьезных вызовов экономической и национальной безопасности в 21-м веке.

В связи с увеличением социальных последствий технологического прогресса и его влиянием, Комитет по правовым и политическим вопросам решил на своем тридцать девятом заседании в Тбилиси 4 апреля 2012 г. рассмотреть проблему кибербезопасности в государствах-членах ЧЭС с точки зрения парламентского вклада в этот процесс.

Поэтому Сороковое заседание Комитета в Афинах 17-18 октября 2012 г. посвящено вопросу «Роль парламентов в укреплении информационной (кибер) безопасности в государствах-членах ЧЭС» и подготовке доклада и рекомендаций для обсуждения на Сороковом пленарном заседании Генеральной Ассамблеи в Баку в ноябре 2012 г.

ПАЧЭС всегда уделяла большое внимание вопросу укрепления информационного общества и технологического развития в рамках деятельности Ассамблеи, в связи с чем были приняты соответствующие доклады и рекомендации[1], в которых подчеркивается важность обеспечения безопасности научных, технологических и новаторских систем, а также разделение ответственности для того, чтобы противостоять потенциальным угрозам в этой сфере и максимально использовать преимущества и возможности, обеспечиваемые информационно-коммуникационными технологиями всем народам в безопасной среде.

В докладе использовалась информация, предоставленная национальными делегациями, Грузии, Румынии, России, Сербии и Украины. Кроме того, справочный материал был получен Международным секретариатом ПАЧЭС из соответствующих источников системы Интернет и публикаций.

II. РОЛЬ ПАРЛАМЕНТОВ В УКРЕПЛЕНИИ ИНФОРМАЦИОННОЙ (КИБЕР) БЕЗОПАСНОСТИ В ГОСУДАРСТВАХ-ЧЛЕНАХ ЧЭС

1. В современном мире киберпространство касается практически всех и каждого. Всемирная сеть представляет собой глобальную информационную систему объединенных компьютерных сетей. Новые информационные технологии сжимают пространство и время, предлагая молниеносный доступ к глобальным знаниям и возможность мгновенного обмена информацией. Однако, такой масштаб

[1] *Доклад и рекомендация 45/2000 «О развитии связи в Черноморском регионе»; Доклад и рекомендация 60/2002 «О глобализации: вызовах и перспективах для государств-членов ПАЧЭС»; Доклад и рекомендация 66/2002 «Об информационном обществе и роли новых технологий»; Доклад и рекомендация 71/2003 «О Черноморском информационном альянсе»; Доклад и рекомендация 95/2007 «О сотрудничестве в области высоких технологий между государствами-членами ЧЭС»; Доклад и рекомендация 121/2011 «О роли парламентов в обеспечении законодательной поддержки укрепления научно-технического прогресса».*

взаимосвязанности также означает, что проблемы, возникшие в одном месте, потенциально могут повлиять и на компьютеры в другом месте, и наряду с динамизмом технологического развития принести с собой сопутствующие проблемы кибербезопасности.

2. Общество и люди никогда не были связаны между собой так, как в наши дни. Сети электронных информационных потоков укоренились почти в каждом сфере нашей жизни. Глобально взаимосвязанная цифровая информация и инфраструктура связи, известная как киберпространство, лежит в основе почти каждой грани современной деятельности и обеспечивает важную поддержку экономике, общественной инфраструктуре, общественной и национальной безопасности. Киберпространство состоит из сотен тысяч взаимосвязанных компьютеров, серверов, маршрутизаторов, переключателей и волоконно-оптических кабелей, обеспечивающих функционирование систем в секторе сельского хозяйства, пищевой промышленности, водоснабжения, общественного здравоохранения, аварийно-спасательных служб, управления, информации и телекоммуникаций, энергетики, транспорта, банков и финансов, почтовых услуг и т.д. Сегодня киберпространство представляет собой основную и контролирующую систему объектов жизнеобеспечения и платформу для новаторских решений и процветания.

3. С другой стороны, компьютеризация и связь влекут за собой наиболее сложные проблемы кибербезопасности. При широком охвате обширной и легко регулируемой электронной инфраструктурой более велики риски для определенных уязвимых объектов. Слаженно функционирующее киберпространство способствует развитию и прогрессу, однако, «кибератаки» могут трансформировать уязвимость компьютерной системы в разрушительную силу и привести к серьёзным последствиям. Для борьбы с подобными атаками необходимо иметь широкие возможности, чтобы соответствующим образом решить проблему уязвимости и сделать так, чтобы как граждане, так и общество в целом смогли реализовать в полной мере потенциал революционных информационных технологий. Поэтому, необходимо усиливать анализ киберугрозы с тем, чтобы понять её долгосрочные тенденции и уязвимость систем.

4. Киберпространство является одним из важных компонентов национальной безопасности. Надёжное и безопасное киберпространство представляет собой сложную стратегическую задачу, требующую координированных и целенаправленных действий со стороны всего общества – государства, частного сектора и народа. Политика в области кибербезопасности должна включать стратегию, тактику и стандарты безопасности операций в киберпространстве, а также охватывать полный спектр действий по снижению угрозы, снижению уязвимости, участию международного сообщества, реагированию на инциденты, связанные с компьютерной безопасностью, повышению способности к восстановлению, политике восстановления и мероприятиям, включая функционирование компьютерных сетей, обеспечение доступности, целостности и безопасности информации, обеспечение соблюдения законов и разведывательные акции поскольку они связаны с безопасностью и и стабильностью глобальной информационно-коммуникационной сети.

5. Для принятия мер по длинному перечню приоритетов в области кибербезопасности, необходимо развивать новаторский подход. Другим вызовом является обеспечение лучшей безопасностью информационных потоков, передаваемых по различным

каналам системы Интернет. Все инженерные подходы к безопасности должны сопровождаться методами мониторинга и быстрого обнаружения любого риска для безопасности. Успех системы кибербезопасности зависит от понимания надёжности всей системы, а не просто защиты её отдельных частей. Следовательно, необходимо принимать комплекс мер по противодействию киберпреступности и кибертерроризму на личном, социальном, политическом уровнях, а также в цифровой среде.

6. Основной обязанностью правительств является устранение уязвимых мест в киберпространстве и ознакомление мировой общественности с полным потенциалом информационной революции. Государства не смогут защитить себя от возрастающей угрозы киберпреступности или вторжений без существенного прогресса в области безопасности этих систем или значительных изменений в том, как они создаются и используются. Государствам необходимо увеличить инвестиции в исследования, которые помогут устранить язвимые места в системе кибербезопасности, удовлетворяя при этом экономические потребности и требования национальной безопасности.

7. Правительствам необходимо объединить сталкивающиеся интересы для того, чтобы выработать целостный подход и план решения проблем, связанных с кибербезопасностью, которые стоят перед странами. Важно выработать политику по снижению рисков, связанных с кибербезопасностью. Также важно больше привлекать внимание общественности к угрозам и рискам, и обеспечивать интегрированный подход к безопасности в киберпространстве.

8. Государства-члены ПАЧЭС, также как и многие другие страны мира, предпринимают всеобъемлющие меры по борьбе с угрозами кибербезопасности. Перед ними стоит угроза двойственного характера: поддержание среды, способствующей новаторству и технологическому развитию, укрепляя при этом надежность и безопасность сетей и неприкосновенность частной жизни.

9. В Румынии, например, парламент принял в 2008 г. закон №298 о борьбе с информационной преступностью, однако в 2009 г. Конституционный суд отклонил его. Он был предан публичному обсуждению, однако в 2011 г. Сенат вновь отклонил этот закон. В 2012 г. Правовой комитет Палаты депутатов внес две поправки в этот закон, он был утвержден Президентом и обнародован. В своей новой версии закон 298/2012 о сохранении общей или обработанной информации государственными телефонными или Интернет-компаниями подчеркивает важность сохранения всего информационного трафика (но не содержания звонков или сообщений) в течение шести месяцев и предоставления этих данных по официальному требованию органам национальной безопасности.

10. В целях решения задач в сфере укрепления информационной безопасности в России, Президентом Российской Федерации была одобрена *«Доктрина информационной безопасности Российской Федерации».* В соответствии с параграфом 1 этой доктрины, информационная безопасность Российской Федерации означает защиту государством своих национальных интересов в информационной сфере наряду с достижением разумного баланса между интересами индивидуума, общества и государства. Информационная безопасность является неотъемлемой частью национальной безопасности России. В 2008 г. Президент Российской Федерации утвердил *«Стратегию развития информационного общества*». Обеспечение

национальной безопасности в информационной сфере является одним из приоритетов страны. Объем управления в области национальной безопасности определяется федеральным конституционным законом «О правительстве Российской Федерации» (ст. 23), федеральным конституционным законом «О судебной системе Российской Федерации», федеральным конституционным законом «О комиссаре по правам человека в Российской Федерации» (ст. 24); федеральным законом «О Федеральной службе безопасности», федеральным законом «О безопасности», федеральным законом «О полиции», федеральным законом «О Счётной палате Российской Федерации» и т.д. Указ Президента Российской Федерации от 30.11.1995 г. №1203 (с поправками, внесенными 21.09.2011) «Об утверждении перечня информации с грифом «государственный секрет» определяет список информации в области военной политики, внешней политики, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности государства, затрагивающей безопасность России. Меры по обеспечению и защите гражданских прав и свобод, прав организаций в области информации определяются законом «О личных данных», законом «О средствах массовой информации», законом «о защите детей от информации, вредной для их здоровья и развития», законом «О связи», законом «О лицензировании определенных видов деятельности», Гражданским кодексом Российской Федерации и т.д.

11. Существующие правовые рамки, регулирующие сферу информационной безопасности в Сербии, включают закон «О конфиденциальности информации» («Официальная газета РС», №104/09), закон «О защите личной информации» («Официальная газета РС», №97/08 и 104/9), закон «Об электронной подписи» («Официальная газета РС», №135/04), закон «Об организации и полномочиях государственных органов власти в борьбе в преступностью в области высоких технологий («Официальная газета РС», №61/05б 104/09), и Уголовный кодекс («Официальная газета РС», №85/05,88/05,107/05,72/09 и 111/09). Правовая база состоит как из закона «Об электронных средствах связи» («Официальная газета РС», №44/10), так и закона «Об обороне» («Официальная газета РС», №116/07,88/09, 104/09). Закон «О конфиденциальности информации» регулирует систему определения и защиты конфиденциальной информации, представляющей интерес для национальной и общественной безопасности Сербии, оборону, внутренние и внешние отношения, защиту иностранной конфиденциальной информации, доступ к конфиденциальной информации и прекращение действия конфиденциальных обязательств, полномочия органов власти и мониторинг исполнения закона, ответственность за неисполнение обязательств, предусмотренных законом, и другие вопросы, относящиеся к защите конфиденциальности. Стратегия развития системы предоставления государственных услуг гражданам и организациям в электронной форме («электронного правительства») в Республике Сербия на период с 2009 по 2013 годы с планом действий по осуществлению мероприятий, предусмотренных этой стратегией («Официальная газета РС» №83/09 и 5/10), рассматривает принцип информационной безопасности в качестве одного из принципов разработки электронного правительства, а план действий по осуществлению мероприятий, предусмотренных этой стратегией, включает подготовку проекта закона об информационной безопасности.

12. В рамках вопроса информационной безопасности в Турции, которая 10.11.2010 подписала Конвенцию Совета Европы о киберпреступности, Министерство транспорта, мореходства и связи Турции подготовило проект Резолюции о

выполнении и координации мер по обеспечению информационной безопасности. Ведомство по информационным технологиям и связям в сотрудничестве с Министерством транспорта, мореходства и связи Турции и Советом по научным и техническим исследованиям Турции (ТУБИТАК), а также при участии ряда других министерств, каждый год организует практические занятия по обеспечению информационной безопасности на национальном уровне. В июле 2012 г. был создан Институт по вопросам информационной безопасности в рамках Центра исследований ТУБИТАК-БИЛГЕМ.

13. Целесообразные законы и правила, касающиеся кибербезопасности, необходимо принимать и обновлять тогда, когда это необходимо, однако одного лишь принятия и осуществления национальных законов недостаточно для решения современных проблем кибербезопасности. Информационные и коммуникационные сети принадлежат и управляются частным сектором как на национальном, так и международном уровнях. Поэтому решение проблем кибербезопасности требует партнерских отношений между государственным и частным секторами, а также международного сотрудничества и норм, которые должны стать ключевым компонентом стратегий по обеспечению кибербезопасности. С течением времени динамика киберпространства требует урегулирования и поправок для внесения в соответствующие стратегии.

14. Подготовлена и ожидает утверждения «Стратегия национальной кибербезопасности Грузии (2012-2015 годы)». В стратегии определяются шаги, которые должны быть предприняты государством, частными компаниями, организациями и отдельными гражданами для улучшения коллективной кибербезопасности, а также определяются меры по снижению уровня уязвимости для атак, направленных на инфраструктуры, содержащие ключевую информацию. Стратегия предусматривает укрепление возможностей правоохранительных органов по предупреждению кибератак и преследованию их исполнителей в судебном порядке; проведение оценок уязвимости национального киберпространства для лучшего понимания потенциальных последствий угроз и уязвимости; создание механизмов в системе Интернет с помощью совершенствования протоколов и маршрутирования; содействие использованию надежных систем электронного контроля/централизованного контроля и систем приёма и накопления данных; сокращение уровня уязвимости программного обеспечения и искоренение имеющихся там недостатков; повышение физической безопасности киберсистем и телекоммуникаций; обеспечение приоритетного характера исследованиям в области кибербезопасности, а также оценку вновь появляющихся систем безопасности. В стратегии также уделяется особое внимание осведомленности, образованию, профессиональной подготовке и международному сотрудничеству в области кибербезопасности с целью содействия обмену информацией, снижению уязвимости, координированию и переориентированию исследований, а также определению и разработки стратегий сдерживания враждебной или вредной деятельности в киберпространстве. Также важно укреплять усилия контрразведки, связанные с кибербезопасностью, улучшать координацию реагирования на кибератаки, содействовать диалогу и установлению партнерских отношений по защите информационной инфраструктуры и развитию глобальной безопасности между государственным и частным секторами на международном уровне, способствовать созданию национальных и международных систем наблюдения и оповещения для обнаружения и предупреждения кибератак по мере их появления

или обеспечению, по крайней мере, всеобъемлющего характера их законов и процедур, а также присоединиться к Конвенции Совета Европы о киберпреступности.

15. Стратегия национальной безопасности Украины «Украина в изменяющемся мире» обеспечивает информационную безопасность и предусматривает создание национальной системы кибербезопасности. Информационная безопасность является одним из приоритетных направлений политики в рамках закона Украины «Об информации». Деятельность по обеспечению безопасности в области систем информации и телекоммуникаций регулируется законом Украины «О защите информации в информативно-телекоммуникационных системах», принятым в 2005 г. Закон Украины «О государственной службе защиты специальной связи и информации Украины» был принят 23 февраля 2006 г. Этот орган регулируется положениями типового закона об информатике и информации, а также соглашением о сотрудничестве между государствами-членами Содружества Независимых Государств в борьбе с компьютерной преступностью. Украина также подписала Ковенцию Совета Европы о киберпреступности.

16. Одним из шести приоритетов «Стратегии развития информационного общества Республики Сербия до 2020 г.» («Официальная газета РС», №51/10) является информационная безопасность. В этой стратегии подчеркивается, что соответствующий уровень информационной безопасности всех форм информационно-коммуникативных технологий является одним из необходимых условий создания устойчивого информационного общества. Первым приоритетом в области информационной безопасности является совершенствование организационно-правовых рамок информационной безопасности. Закон о конфиденциальности информации предусматривает принятие нормативов, более чётко регулирующих меры по защите информационных и телекоммуникационных систем, тем не менее, есть необходимость регулирования этого вопроса с помощью закона, поскольку необходимо создать организационно-правовые рамки и определить полномочия некоторых органов, такие как аккредитация систем ИКТ для передачи, получения и хранения конфиденциальной информации, предоставление права на доступ к шифрованной продукции и осуществления технического надзора в области информационной безопасности. Требования к системам ИКТ по работе с конфиденциальной информацией предусматривают создание системы последующего и предшествующего контроля условий для обеспечения удовлетворительного уровня их применения на практике. Специальная рабочая группа, созданная министерством культуры, информации и информационного общества, разработала проект закона об информационной безопасности, нацеленного на укрепление информационной безопасности и регулирование безопасности всего информационного пространства, и, в частности, следующее: информационная безопасность систем ИКТ для работы с конфиденциальной информацией (выдача разрешений для систем ИКТ по работе с конфиденциальной информацией, использование криптографической продукции с целью защиты конфиденциальной информации, защита информационно-коммуникационных систем против вредного электромагнитного излучения, передача обязанностей, требующих опыта в вышеупомянутых сферах деятельности, Совету по национальной безопасности и министерству обороны); информационная безопасность других систем ИКТ, установленных в органах власти; координирование предупреждения и защиты от рисков в области безопасности всех

информационно-коммуникационных систем Республики Сербия; национальные сети связи (установка и эксплуатация академической сети Сербии, а также установка и эксплуатация национальной сети связи); инспекция информационного общества. Проект закона в настоящее время согласуется с государственными структурами, чья деятельность связана с вопросами, регулируемыми этим законом. Правила безопасности и защиты информационных систем государственных органов власти («Официальная газета РС», №41/90) определяют организационные и технические меры обеспечения и защиты информационных систем государственных органов власти на компьютерной основе.

17. В России на национальном уровне была принята национальная программа «Информационное общество (2011 г.-2020 г.), где говорится о том, что из-за отсутствия интегрированного подхода к решению проблемы формирования и развития информационного общества, угрозы безопасности в области информационного общества постепенно возрастают. Приоритеты суб-программы 5 «Безопасность в информационном обществе до 2015 г.» включают следующие меры: создание системы определения и мониторинга уровня реальной защиты информационного общества от терроризма в области информации; создание и развитие внутренних технологий безопасности для хранения и обработки больших объемов неструктурированной информации, включая создание внутренних защищённых функциональных услуг и компонентов процесса, отвечающих за хранение и обработку больших объемов неструктурированной информации, и и их постоянная поддержка и развитие, позволяющая увеличить объемы обработки неструктурированной информации; развитие и интегрирование с системами информационного контроля других отделов и структур общего банка данных, касающихся вопросов борьбы с терроризмом; создание национальной платформы программного обеспечения (комплексные решения внутреннего программного обеспечения – модули, построенные на базе общих технологий, позволяющие разрабатывать новые продукты по схеме и конфигурации готовых модулей, а также совершенно новые продукты), развитие супервычислительных и сетевых технологий. Указом Президента Российской Федерации от 8 февраля 2012 г. №146 «О федеральных структурах исполнительной власти, отвечающей за обеспечение информационной безопасности информационных систем, созданных с использованием суперкомпьютеров и сетевых технологий» были созданы федеральные службы по обеспечению безопасности информации в информационных системах с использованием суперкомьютеров и сетевых технологий – Федеральная служба безопасности Российской Федерации и Федеральная служба технического и экспортного контроля (ФСТЭК Россия). В обязанности «ФСТЭК Россия» входит обеспечение безопасности информации в информационно-телекоммуникационной инфраструктуре, что очень важно для национальной безопасности в сфере информации.

18. Важными обязанностями в деле обеспечения кибербезопасности является подготовка всеобъемлющего национального плана по обеспечению ключевых ресурсов и ключевой инфраструктуры; обеспечение антикризисного управления в ответ на атаки на ключевые информационные системы; оказание технической помощи частному сектору и правительственным структурам в отношении планов восстановления во время сбоя ключевых информационных систем; координирование деятельности с другими структурами правительства по обеспечению специального оповещения и предоставлению консультаций о соответствующих мерах защиты и

контрмерах государственным, местным и межправительственным организациям, включая частный сектор, научные круги и общественность; проведение и финансирование исследований и разработок наряду с другими агентствами, что приведет к новому научному мышлению и технологиям в области безопасности. Координирование деятельности государственных, местных и неправительственных организаций, включая частный сектор, научные круги и общественность, имеет очень важное значение.

19. Защита широко распространенных объектов киберпространства требует усилий многих стран и граждан. Одни только правительства не смогут достаточно надежно защищать киберпространство. Большинство объектов ключевой инфраструктуры и киберпространство, которое они используют, находится и управляется частным сектором. Технологии, создающие и поддерживающие киберпространство, стремительно развиваются с помощью частного сектора и научных инноваций. Необходимы совместные действия, поскольку технологии развиваются, угрозы и уязвимость систем меняются и формируется понимание проблем киберпространства. Необходимы координированные усилия для определения и исправления самых серьезных проблем уязвимости с помощью совместных усилий, таких как обмен передовым опытом, оценка и использование новых технологий.

20. Инвестиции в безопасность киберпространства будут способствовать развитию рынка для более надежных технологий с помощью крупных закупок передовых технологий по защите информации. Это поможет обеспечить надёжность компьютерных систем и сетей. Страны должны быть в состоянии защитить себя и свои ключевые системы.

21. Экономика и национальная безопасность становятся зависимы от информационных технологий и информационной инфраструктуры. Сеть сетей поддерживает деятельность всех секторов экономики: энергетику (электроэнергия, нефть и газ), перевозки (железнодорожные, воздушные, морские), финансы и банковское дело, информацию и телекоммуникации, государственное здравоохранение, службы экстренной помощи населению, водоснабжение, химическое производство, оборону, промышленность, пищевую промышленность, сельское хозяйство и почтовые услуги. Она также контролирует электрические трансформаторы, трубопроводные насосы, химические резервуары, радары и т.д.

22. Поэтому кибератаки на информационные сети могут привезти к серьёзным последствиям для ключевой деятельности. В целях противостояния подобным атакам и снижения уровня уязвимости необходимо разрабатывать интегрированные программы готовности. Для создания системы постоянного контроля безопасности, проводимого опытными профессионалами, и многослойной и безотказной сети защиты для устранения наиболее серьезных уязвимых мест, необходимо постоянно проводить оценку уязвимости сети и мероприятия по устранению её недостатков. Противостояние угрозам и снижение уровня уязвимости киберпространства является особенно сложной проблемой. Для обеспечения безопасности киберпространства необходимы действия на различных уровнях с участием разных действующих групп.

23. Несмотря на повышенную осведомленность о важности кибербезопасности и мерах по повышению её возможностей, киберриски продолжают лежать в основе информационных сетей и систем. К сожалению, нет одной отдельной стратегии, способной полностью устранить риски киберпространства и связанные с этим

угрозы. Защита киберпространства - продолжающийся процесс, поскольку появляются новые технологии, а вместе с ними появляются и новые уязвимые места.

Роль национальных парламентов

24. Национальные парламенты должны добавить свой голос к решению проблем безопасности киберпространства и внести свой вклад в расширение мер обеспечения безопасности информации в государствах-членах ЧЭС, как важного элемента достижения устойчивого развития.

25. Главной задачей национальных парламентов является надзор за деятельностью правительств в процессе выработки всеобъемлющего национального плана защиты ключевых ресурсов и ключевой инфраструктуры, включая информационную технологию и системы телекоммуникации с целью предотвращения возможных кибератак.

26. Также важно продолжать повышать уровень гармонизации соответствующего законодательства с международными стандартами в сфере кибербезопасности.

27. Парламенты должны тщательно определять приоритеты финансирования в науку, технологию и инновации для развития, стимулирования и расширения исследований с тем, чтобы удовлетворять национальным приоритетам и стратегическим задачам в сфере кибербезопасности.

28. Парламентарии должны максимально использовать имеющиеся правовые механизмы с целью выработки всеобъемлющей национальной ознакомительной программы обеспечения безопасности киберпространства для того, чтобы преимущества технологического развития были поняты и получили широкую поддержку, снижая при этом до минимума и смягчая ущерб от возможных кибератак.

29. Также необходимо установить систему так называемой «глубокой обороны», состоящей из многослойных систем безопасности, использующих меры по защите информационных ресурсов и предупреждению несанкционированного доступа к информации.

30. Также необходимо проводить работу по определению взаимоприемлемых условий функционирования сети международных центров по предупреждению и отражению кибератак с целью создания надежных механизмов по обмену информацией и опытом в области кибербезопасности.

31. Особое внимание следует уделять взаимодействию и координированию деятельности правоохранительных органов, разведывательных служб, судебных органов в целях их соответствующей подготовки для борьбы с кибератаками и вторжениями в киберпространство.

32. Парламенты должны возглавить процесс выработки международной стратегии для объединенного отражения киберугрозы и создания общих международных правовых механизмов с целью гармонизации национального уголовного законодательства в этом отношении.

33. Парламенты должны разрабатывать правила с целью обеспечения поддержки частному сектору для хорошо координированного осуществления практических мер

по обеспечению безопасности информации путем создания и применения наиболее передовых технологий.

34. Парламенты должны также прилагать усилия по укреплению рамок участия в выработке международных стандартов в области информационной безопасности с целью прогнозирования, раннего и своевременного диагностирования, научной и технологической экспертизы, своевременного обнаружения новых факторов риска с целью сокращения уязвимости и отражения угроз в киберпространстве.

35. Парламенты должны также принимать активное участие в ратификации международных инструментов, касающихся устойчивого развития на основе научно-технологического прогресса и включать эти положения в национальное законодательство.

36. Парламентская Ассамблея Черноморского Экономического Сотрудничества должна оказывать поддержку мероприятиям ЧЭС, направленным на расширение многостороннего сотрудничества в области науки и технологии, и установить тесные контакты с Рабочей группой по науке и технологии.

Международное сотрудничество

37. Одним из главных инструментов укрепления международной кибербезопасности является Конвенция Совета Европы о киберпреступности, принятая в 2001 г. В ней даются рекомендации о гармонизации национальных правовых рамок и элементах международного сотрудничества в борьбе с киберпреступностью. Этот правовой инструмент имеет как практическое, так и политическое значение. В связи с тем, что он рекомендует пути развития соответствующих национальных правовых рамок борьбы с киберпреступностью, этот документ является полезным инструментом экспорта европейских норм по этому вопросу. Более того, присоединение к Конвенции содействует международному сотрудничеству по оперативным вопросам, за исключением экстрадиции киберпреступников. Политическое значение Конвенции заключается в том, что она является единственным международным соглашением по вопросам кибербезопасности, обязательным для исполнения, а присоединение к Конвенции говорит о том, что страна готова гармонизировать свои внутренние законы и серьезно бороться с киберпреступностью. Совет Европы наряду с частным сектором и государствами-членами начал осуществление глобального проекта по борьбе с киберпреступностью с целью осуществления конвенции во всем мире. Возрастающее число стран, присоединяющихся к Конвенции, обеспечивает существенное сдерживание криминальных групп и правительств, спонсирующих кибератаки через прокси-объекты на своих территориях.

38. Межправительственная Рабочая группа по информационной безопасности и неприкосновенности частной жизни при Организации Экономического Сотрудничества и Развития (ОЭСР) разрабатывает рекомендации и доклады по созданию информационного общества и отказоустойчивости. С помощью экспертов из правительственных, деловых кругов и гражданского общества она осуществляет мониторинг тенденций и содействует обмену информацией. ОЭСР регулярно подготавливает доклады, содержащие анализ влияния технологии на информационную безопасность и неприкосновенность частной жизни. Доклад ОЭСР о практике защиты ключевой информации и инфраструктуры (CIIP) в государствах-членах является одним из лучших сравнительных документов в этой области,

содержащим анализ передового опыта, организационных структур и правил, установленных в большинстве развитых стран. Докладом «Снижение системных рисков кибербезопасности» ОЭСР начала публикацию серии материалов о результатах исследований под названием «Глобальные шоки». В связи с тем, что кибербезопасность в контексте ОЭСР является главным образом подкатегорией экономической и технологической политики, подъем проблемы кибербезопасности до уровня национальной безопасности несколько снизил её значение на повестке ОЭСР. Вклад ОЭСР в обобщение и распространение передового опыта в развитии безотказности национальной информационной инфраструктуры может быть полезен для стран, занимающихся поиском подходящей модели для своих национальных структур, отвечающих за кибербезопасность.

39. Организация по безопасности и сотрудничеству в Европе (ОБСЕ) начала обсуждение вопросов кибербезопасности в 2008 г. С того времени государства-участники ОБСЕ провели несколько заседаний на высоком уровне по кибербезопасности, где центральными темами для обсуждения было повышение осведомленности о кибербезопасности, потребность стран в создании ресурсов для борьбы с киберпреступностью и терроризмом, а также определение ответственного государственного поведения в киберпространстве. Страны ОБСЕ имеют различные интересы и точки зрения по вопросу безопасности киберпространства, и до сих пор не было достигнуто консенсуса по вопросу о конкретной роли ОБСЕ в этих дебатах. Совместное заседание Форума ОБСЕ по сотрудничеству в области безопасности и Постоянного Совета ОБСЕ, состоявшееся в июне 2010 г., решило продолжить дискуссии по стратегическим вопросам кибербезопасности.

40. Генеральная Ассамблея ООН приняла резолюции по кибербезопасности. В рамках Социально-экономического Комитета ООН были приняты резолюции 56/121 «Об уголовно наказуемом злоупотреблении информационной технологией» и 57/239 «О создании глобальной культуры кибербезопасности». В обеих резолюциях подчеркивается значение международного сотрудничества, необходимость искоренения надёжных убежищ для киберпреступников, поощрение сотрудничества между правоохранительными органами, а также повышение общей осведомленности о вопросах кибербезопасности. Резолюция 64/422 «О глобализации и взаимозависимости: наука и технология во имя развития» также включает обзор самооценки защиты ключевой информационной инфраструктуры для стран ООН с целью повышения их киберзащиты. Эти инициативы привлекли внимание к возрастающей обеспокоенности в связи с киберугрозами, помогли поднять глобальную осведомленность, а также стимулировать страны ООН к принятию необходимых мер по совершенствованию своих национальных механизмов, обеспечивающих кибербезопасность. Резолюция ООН №64/386 «О событиях в области информации и телекоммуникациях в контексте международной безопасности», принятая в 2009 г., предлагает продолжить дискуссии по кибербезопасности в контексте международной безопасности и создать группу экспертов, которая подготовит дальнейшие рекомендации. В 2010 г. группа правительственных экспертов ООН в области последних событий в сфере информации и телекоммуникаций в контексте международной безопасности подготовила доклад, в котором к странам обращаются с призывом к сотрудничеству с целью повышения информационной безопасности и укрепления международного сотрудничества. В докладе даются рекомендации по дальнейшему межгосударственному диалогу о снижении рисков и защите ключевой национальной

и международной инфраструктуры. Следует отметить, что 12 сентября 2011 г. постоянные представители Китая, России, Таджикистана и Узбекистана в ООН направили совместное письмо Генеральному секретарю ООН с просьбой разослать проект «Правил поведения в области обеспечения международной информационной безопасности». Основной задачей этих правил является выработка кодекса ответственного поведения государств в сфере международной информационной безопасности с учетом военных, политических, криминальных и террористических вызовов и угроз. В документе говорится о борьбе с использованием информационно-коммуникативных технологий, не имеющим ничего общего с задачами достижения международной стабильности, укрепления мира и безопасности. В нем также предусматривается соблюдение прав человека и основных свобод в информационном пространстве, уважение суверенитета, территориальной целостности и политической независимости всех государств, а также создание многостороннего прозрачного и демократичного международного механизма регулирующего систему Интернет. Российская Федерация, как один из разрабочиков этого проекта, призывает все заинтересованные стороны принять активное участие в обсуждении этого вопроса. Эта инициатива может стать первым шагом по пути выработки всеобщего документа ООН – Конвенции, которая будет направлена на обеспечение всесторонней международной информационной безопасности, как можно шире учитывающей интересы мирового сообщества.

41. НАТО разработал свою первую политику в области кибероборонs в 2007 г., которая служит основой для других стратегических документов и деятельности в этой области. НАТО был первой международной организацией, быстро адаптировавшейся к новой стратегической среде и признавшей, что противостояние нетрадиционным угрозам безопасности имеет основное значение для национальной безопасности союзников. Политика НАТО в области кибероборонs, принятая в 2007 г., определила задачи расширения возможностей кибероборонs собственных сетей НАТО и создала первоначальные механизмы для консультаций с государствами-членами по вопросам кибероборонs. Технический центр НАТО для нанесения ответного удара в случае компьютерной атаки служит центральным техническим органом, уполномоченным решать оперативные вопросы кибероборонs. Протоколы о намерениях в области кибероборонs способствуют проведению регулярных консультаций, обмену информацией и дают описание того, как группы быстрого реагирования НАТО могут оказать помощь отдельным членам Альянса в случае киберкризиса. В новой стратегической концепции НАТО, принятой на Лиссабонском саммите в ноябре 2010 г., подчеркивается, что НАТО должен ускорить принятие мер в ответ на угрозу кибератак. На Лиссабонском саммите перед НАТО и членами Альянса поставили задачу противостояния новым вызовам безопасности и, среди других задач, была подготовлена весьма амбициозная «дорожная карта» для киберповестки Альянса. Она предусматривает подведение всех военных и гражданских структур НАТО под центральную защиту, включение киберкомпонента в процесс планирования обороны и ускорение обмена информацией, а также возможности раннего оповещения. В июне 2011 г. министры обороны НАТО утвердили политику НАТО в области кибероборонs, где предусматриваются усилия в области кибербезопасности, а также план действий. В мае 2012 г. в Чикаго главы государств и правительств приняли решение объединить все сети НАТО для централизованной защиты в рамках нанесения ответного удара НАТО в случае компьютерной атаки.

42. ЕС подходит к вопросу кибербезопасности фрагментарно, при этом параллельно проводится политика с различными пересекающими темами. Большая часть этих инициатив имеет прямое или косвенное отношение к готовности членов ЕС к отражению серьезных кибератак, т.к. они касаются способов и методов кибератак, а также их последствий. В 2007 г. Европейская Комиссия подготовила документ «Об общей политике в борьбе с киберпреступностью», в котором говорится об улучшении оперативного сотрудничества правоохранительных органов, сотрудничестве в области политике и координации между государствами-членами. В нем также говорится о развитии сотрудничества в политической и правовой сферах с третьими странами и повышении осведомленности – профессиональной подготовке, исследованиях и укреплении диалога с промышленностью для возможных законодательных мер. «Антирадикализация», т.е. способность осуществлять мониторинг и оценивать острый идеологический материал, уже давно находится в центре внимание антитеррористических стратегий ЕС. В декабре 2009 г. была принята «Стокгольмская программа», представляющая собой значительный шаг в повестке «внутренней безопасности» Европейского Союза. Кроме призыва к выработке европейской стратегии внутренней безопасности программа несколько раз упоминает о кибербезопасности, включая необходимость принятия лучших и более широких мер для обеспечения устойчивой безопасности информационных сетей, лучшую способность противостоять кибератакам, важность ратификации всеми государствами-членами конвенции о борьбе с киберпреступностью, и значение обмена информацией как между правительствами, так и частным сектором. Принятая в октябре 2010 г. новая стратегия внутренний безопасности ЕС нацелена на повышение уровня безопасности в киберпространстве как граждан, так и предприятий, а также принятие мер по оперативному решению проблем киберпреступности. Три конкретных предложения, указанные в стратегии, включают создание к 2013 г. Центра ЕС по борьбе с киберпреступностью, создание до 2012 г. сети групп ликвидации аварийных ситуаций в компьютерной сети во всех институтах ЕС (включая сотрудничество этих институтов с правоохранительными органами), и создание к 2013 г. Европейской системы оповещения и обмена информацией. В 2010 г. Совет согласовал План борьбы с киберпреступностью, в котором также говорится об укреплении европейской платформы борьбы с киберпреступностью при Европоле (ЕССР), оказании лучшей поддержки трансграничной подготовке правоохранительных органов и лучшей международной координации. Европол зачастую оказывается в центре многих новых решений и рекомендаций Совета, а ЕССР недавно была повышена до уровня полноценной инициативы с рядом подчиненных структур. Важная организационная инициатива – Европейский центр по борьбе с киберпреступностью – неоднократно предлагалась и согласовывалась с тех пор, как впервые была обсуждена в 2007 г. В июне 2010 г. было достигнуто соглашение о создании оперативной группы Европейского Союза по борьбе с киберпреступностью в качестве предварительной организации, действующей до фактического открытия Центра.

III. ВЫВОДЫ

43. За последние несколько лет резко возросли угрозы безопасности киберпространства. Учитывая возрастающую зависимость от киберпространства практически в каждой сфере жизни, страны и международные организации начали разрабатывать политику по защите функционирования информационных систем и обеспечению противодействия угрозам кибербезопасности.

44. Поскольку мир стремительно впадает в зависимость от Интернета, обязательства по созданию более защищенной киберсреды становятся велением времени. Возможности «Всемирной паутины» в частной и профессиональной среде практически безграничны. Интернет используется для связи, исследований, торговли и работы. В то же время, системы промышленного контроля, используемые в жизненно важных секторах экономики, также связаны с Интернетом. Это добавляет новое измерение зависимости от Интернета: надёжность и безопасность.

45. Надёжная система Интернета имеет огромное значение для экономики и общества. Постоянно передаётся информация. Инфраструктура, с помощью которой создаётся киберпространство носит глобальный характер своей структуры и развития. В киберпространстве национальные границы не имеют значения. В силу глобального характера киберпространства, имеющаяся уязвимость распространяется на весь мир и доступна в любом месте для каждого, имеющего достаточно способностей её использовать.

46. Страны сталкиваются с двойным вызовом поддержания среды, способствующей инновациям и технологическому развитию, укрепляя при этом безопасность, надёжность и право неприкосновенности частной жизни. Обеспечение кибербезопасности в настоящее время является главным вызовом для государств, предпринимателей и общества как на национальном, так и международном уровне.

47. Каждая страна должна определить соответствующее государственное поведение в киберпространстве, инвестировать в необходимые навыки и образование для того, чтобы люди могли работать в зоне информационной безопасности, а также обеспечивать сотрудничество между государственным, частным и научным секторами. Использование программ по борьбе с угрозами кибербезопасности и снижению уровня уязвимости, а кроме того, повышение осведомленности о безопасности киберпространства и проведение профессиональной подготовки являются велением времени.

48. Для защиты Интернета и других информационно-технологических сетей от угроз и уязвимости, а также с целью дальнейшего сотрудничества на национальном и международном уровнях, национальные парламенты должны способствовать улучшению координации и сотрудничества между государствами в борьбе с использованием информационных технологий в преступных целях, и в этом контексте следует подчеркивать роль, которую могли бы играть международные и региональные организации.

49. Возрастающее количество атак на киберсети стало одной из наиболее серьёзных угроз для обеспечения безопасности социальных сетей и киберпространства. Это говорит о необходимости надёжного, безопасного и отказоустойчивого киберпространства, а также о распространении знаний о киберпространстве и инноваций.

50. Вовлечение государственного и частного секторов является ключевым компонентом обеспечения кибербезопасности. Участие государственных и частных фирм в решении проблем осведомленности, профессиональной подготовки, технологических улучшений, устранения уязвимости и восстановления может принимать различные формы. Мероприятия должны быть также направлены на оказание поддержки исследованиям и развитию технологии, которые смогли бы

защитить сети и системы, указывать на проблемы и оповещать, а также защищать от организованных атак.

51. Необходимо обеспечить конфиденциальность и безопасность использования информационно-коммуникационных технологий, являющихся краеугольным камнем информационного общества. Следует стимулировать, пропагандировать, развивать и решительно внедрять глобальную культуру кибербезопасности.

52. Государства-члены ЧЭС должны более тесно сотрудничать для того, чтобы выработать общую правовую базу в области борьбы с киберпреступностью, а также развивать совместные действия по защите информационных сетей. Государства-члены ЧЭС, которые не являются членами ЕС, должны работать в сотрудничестве с государствами-членами ЧЭС, которые являются членами ЕС с целью принятия общего законодательства.

53. Страны должны инвестировать в передовые исследования, необходимые для инноваций и открытий, чтобы противостоять цифровым вызовам нашего времени; делать пропорциональные инвестиции в безопасность сетей, техническую подготовку, ознакомление с вопросами кибербезопасности и компьютерную грамотность.

54. Всё возрастающий объем и сложность угроз кибербезопасности, таких как афёры, кража информации и другие виды уязвимости сети, требуют от пользователей бдительности в вопросе защиты своих сетей и информации. Необходимо, чтобы каждый пользователь понимал риски, а также необходимые действия по защите информационных и киберсетей.

55. Во взаимосвязанном мире с наличием мириад устройств, таких как компьютеры, смартфоны, планшетные компьютеры, все пользуются одним и тем же каналом связи и каждый пользователь имеет свою роль в обеспечении безопасности своего киберпространства. Защита Интерната и других цифровых ресурсов является общей ответственностью каждого пользователя любого вида. Учитывая то, что люди с удовольствием пользуются Интернетом и ценят те возможности, которые он привносит в их жизнь, необходимо помнить о том, что кибербезопасность начинается с ответственного поведения в киберпространстве каждого отдельного пользователя.