ПАРЛАМЕНТСКАЯ АССАМБЛЕЯ ЧЕРНОМОРСКОГО ЭКОНОМИЧЕСКОГО СОТРУДНИЧЕСТВА
ПАЧЭС

МЕЖДУНАРОДНЫЙ СЕКРЕТАРИАТ

Док.: GA51/LC51/REP/18/r

КОМИТЕТ ПО ПРАВОВЫМ И ПОЛИТИЧЕСКИМ ВОПРОСАМ

ДОКЛАД [*]

УКРЕПЛЕНИЕ СОТРУДНИЧЕСТВА В ОБЛАСТИ КИБЕРБЕЗОПАСНОСТИ В ГОСУДАРСТВАХ-ЧЛЕНАХ ЧЭС

Докладчик: г-н Эльдар ГУЛИЕВ, заместитель Председателя Комитета,
(Азербайджан)

[*] *Текст рассмотрен на Пятьдесят первом заседании Комитета по правовым и политическим вопросам в Тиране 19 июня 2018 г. и утвержден на Пятьдесят первой Генеральной Ассамблее в Тиране 20 июня 2018 г.*

I. ВСТУПЛЕНИЕ

1. 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. Новые информационные технологии сжимают пространство и время, и создают возможность широкого доступа к глобальным знаниям и обмену информацией.

2. Ведущие страны мира уже перешли на использование таких понятий, как е-правительство, е-подпись, цифровая экономика и др. Компьютеры, смартфоны, планшеты и другие устройства являются носителями и хранителями важной государственной и конфиденциальной информации, а также позволяют обмениваться информацией в считанные секунды, вести государственные и банковские дела, совершать покупки в Интернете, оплачивать услуги при помощи кредитной карты или виртуальных денег. Эти устройства также являются хранилищем ценной информации: государственных документов, материалов и других важных конфиденциальных данных. Из года в год возрастает зависимость жизненно важных направлений общества от информационных технологий практически в любой сфере, и поэтому проблемы, связанные с безопасностью киберпространства, приобретают глобальный характер.

3. С каждым днем растет количество случаев кибертерроризма, киберпреступности и кибератак на фоне развития информационных технологий и технологического прогресса. Это ведет к беспокойству стран, больших корпораций и населения в отношении преступлений в киберпространстве, совершаемых неизвестными нарушителями и хакерами, нападающими на стратегически важные компьютерные сети и программы.

4. Поэтому Комитет по правовым и политическим вопросам решил на своем пятидесятом заседании в Ростове-на-Дону 25 октября 2017 г. рассмотреть проблему кибербезопасности в государствах-членах ЧЭС. Пятьдесят первое заседание Комитета посвящено вопросу «Укрепление сотрудничества в области кибербезопасности в государствах-членах ЧЭС» и подготовке доклада и рекомендаций для обсуждения на Пятьдесят первом пленарном заседании Генеральной ассамблеи в Тиране в июне 2018 г.

5. ПАЧЭС уже рассматривала вопрос кибербезопасности в 2012 году на Сороковом пленарном заседании Генеральной Ассамблеи в Баку, обращая внимание на роль парламентов в укреплении сотрудничества в этой области. В принятых документах подчеркивается важность разделения ответственности с целью противостоять потенциальным угрозам и максимально использовать преимущества и возможности, обеспечиваемые информационно-коммуникационными технологиями в безопасной среде, как важного элемента достижения устойчивого развития. В документах 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.

6. В настоящем докладе используется информация, предоставленная национальными делегациями Азербайджана, Болгарии, Грузии, Греции, Молдовы, Румынии, Сербии, Турции и Украины. Кроме того, справочный материал был получен Международным секретариатом ПАЧЭС из соответствующих источников системы Интернет и публикаций.

II. УКРЕПЛЕНИЕ СОТРУДНИЧЕСТВА В ОБЛАСТИ КИБЕРБЕЗОПАСНОСТИ В ГОСУДАРСТВАХ-ЧЛЕНАХ ЧЭС

7. Кибербезопасность является совокупностью средств и стратегий, направленных на обеспечение безопасности информационных сетей и данных, от несанкционированного доступа. Элементы кибербезопасности включают в себя: контроль доступа, обучение персонала, отчётность, оценку вероятных рисков, тестирование на проникновение и требование авторизации. Одним из наиболее проблемных элементов кибербезопасности является быстрый и постоянно меняющийся характер угроз сохранности сферы телекоммуникаций. Традиционный подход концентрирует ресурсы на наиболее важных компонентах информационной безопасности и защищает от угроз хакерских атак. Поэтому, кибербезопасность сегодня является необходимым условием дальнейшего развития и укрепления информационного общества.

8. Киберпространство состоит из глобальных компьютерных сетей, которые соединяются и контролируются при помощи кабельных, оптоволоконных и беспроводных соединений. Киберпространство объединяет Интернет и транснациональные сети, занимающиеся передачей данных в разных областях. Существуют также системы, получающие и контролирующие данные путем «общения» машин через панельные управления и радиочастотную идентификацию, которые называются «интернетом вещей». Угрозы в киберпространстве многообразны, как и само киберпространство, что требует их тщательного изучения и противостояния им.

9. В современном мире киберпространство касается практически всех и каждого, кто является частью глобальной информационной системы, объединяющей компьютерные сети. 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. Сотни тысяч взаимосвязанных компьютеров, серверов, маршрутизаторов, переключателей и волоконно-оптических кабелей обеспечивают 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. Все это требует постоянного контроля и изучения этих систем.

10. Социальные сети – это еще одно быстро развивающееся направление, которое предоставило человечеству новые возможности общения и обмена информацией. Однако и здесь необходимо обеспечение кибербезопасности для защиты систем от неавторизованного использования баз данных и накопленной информации личностного характера.

11. Общество и люди никогда не были связаны между собой так, как в наши дни. Сети электронных информационных потоков укоренились почти в каждой сфере жизнедеятельности. Сегодня киберпространство представляет собой основную и контролирующую систему объектов жизнеобеспечения. При широком охвате обширной и легко регулируемой электронной инфраструктурой велики риски для определенных уязвимых объектов. В контексте глобального роста влияния информационных технологий безопасность в этой сфере становится главным вызовом для мирового сообщества, каждого отдельно взятого государства и каждого человека. Поэтому, одной из главных задач является сведение к минимуму рисков в этой сфере.

12. Существующий широкий масштаб взаимосвязанности 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. Современные хакеры располагают беспрецедентно широким набором инструментов и способны применять его с максимальной эффективностью. Постоянный рост объемов онлайн-трафика и количества мобильных устройств порождают широкий выбор мишени и средств ее поражения. В таком случае необходимо построить эффективную защиту от постоянно развивающихся и усложняющихся современных угроз. Вредоносные программы позволяют злоумышленникам получить быстрый доступ к незащищенному устройству и похитить любые данные. Современные технологии позволяют пересылать и контролировать нелегальные финансовые потоки, что является основой современного терроризма. Современный террорист может причинить значимый ущерб с помощью простой клавиатуры. Поэтому укрепление кибербезопасности и безопасности информационно-коммуникационных технологий является важной задачей для всего мира. Следовательно, с увеличением числа террористических атак, должны развиваться методы их блокирования и предотвращения.

13. Исследователи безопасности из компании «Cisco» опубликовали Отчет[1] по информационной безопасности за 2018 год, в котором предоставили данные и анализ поведения киберпреступников за последние годы. Согласно отчету, одной из наиболее значительных тенденций в 2017 году стала эволюция вредоносного программного обеспечения (ПО), позволяющая получать доступ к существующим данным или их удалять. Исследователи также обратили внимание на появление киберугроз, способных обходить сложные среды песочниц (sandbox) и использовать шифрование для ухода от обнаружения. По данным «Cisco», по состоянию на октябрь 2017 года в зашифрованном виде было передано около 50% глобального web-трафика. При этом анализ более чем 400 тыс. вредоносных двоичных кодов показал, что по состоянию на октябрь 2017 года в около 70% трафика использовалось шифрование в том или ином виде.

14. Согласно отчету «Cisco», одной из основных проблем в области защиты от киберугроз являются атаки с помощью IoT-устройств (Internet of Things) и облачных сервисов. В документе говориться, что IoT-устройства работают круглосуточно и могут быть введены в действие для выполнения вредоносной активности практически моментально. А по мере того, как злоумышленники увеличивают размер своих ботнетов (Botnet), они используют сложные коды и вредоносное ПО, что позволяет организовывать еще более усовершенствованные сетевые DoS-атаки (Denial of Service).

15. Ботнет - компьютерная сеть из устройств, зараженных вредоносной программой. Бот – это скрытая программа, которая устанавливается на вычислительное устройство жертвы с целью его несанкционированного использования. Для получения управления компьютерным устройством на него скрытно устанавливаются программы-бот, которые трудно обнаружить при выполнении привычной ежедневной работы. Проникновение бота может случиться при недостаточной бдительности пользователя, так как автономная программа маскируется под полезное ПО. Боты самостоятельно, без ведома пользователя запускаются на устройстве и защищаются от удаления. Механизм защиты заключается в применении нетрадиционных способов запуска,

---

[1] Годовой отчет по компании «Cisco» кибербезопасности (https://www.cisco.com)

замене файлов системы, перезагрузке машины при доступе к ключам автоматической загрузки. Ботнеты эффективны для работы киберпреступников и трудно уязвимы, поскольку с вредоносными компьютерными устройствами мошенники могут анонимно руководить с любой точки земного шара.

16. В связи с ростом сложности и расширением аналитических возможностей инфраструктур безопасности, все больше исследователей предлагают использовать искусственный интеллект и машинное обучение. По данным «Cisco», 39% специалистов по безопасности полностью полагаются на технологии автоматизации, 34% - на машинное обучение и 32% - на искусственный интеллект. Для защиты от киберугроз, специалисты рекомендуют постоянно корректировать и по возможности устранять уязвимости, регулярно делать резервные копии данных, а также внедрять усовершенствованные технологии безопасности, включающие машинное обучение и способности искусственного интеллекта.

17. Слаженно функционирующее киберпространство способствует развитию и прогрессу, однако, кибератаки могут трансформировать уязвимость компьютерной системы в разрушительную силу и привести к серьезным последствиям. Участились атаки на объекты критической инфраструктуры. Для борьбы с подобными атаками необходимо иметь широкие возможности, чтобы соответствующим образом решить проблему уязвимости.

18. Киберпространство является одним из важных компонентов национальной безопасности. Обеспечение надежности и безопасности киберпространства представляет собой сложную стратегическую задачу, требующую координированных и целенаправленных действий со стороны всего общества – государства, частного сектора и населения. 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 компьютерной безопасности, гарантированию доступности, целостности и безопасности информации, обеспечение соблюдения законов и разведывательные акции поскольку все это связано с безопасностью и стабильностью глобальной информационно-коммуникационной сети.

19. Другим вызовом является обеспечение безопасностью информационных потоков, передаваемых по различным каналам системы Интернет. Все инженерные подходы к безопасности должны сопровождаться методами мониторинга и быстрого обнаружения любого риска. Успех системы кибербезопасности зависит от понимания надежности всей системы, а не просто защиты ее отдельных частей. Следовательно, необходимо принимать комплекс мер по противодействию киберпреступности и кибертерроризму на индивидуальном, социальном, политическом уровнях, а также в киберсреде в целом.

20. Основной обязанностью правительств является устранение уязвимых мест в киберпространстве. Однако 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 уязвимые места в системе кибербезопасности, удовлетворяя при этом требования национальной безопасности.

21. Международный союз электросвязи (ITU) ежегодно публикует исследование «Глобальный индекс кибербезопасности». По результатам опроса оценивается уровень

кибербезопасности государств по пяти основным показателям: законодательная база, технические данные, организационные вопросы, повышение качества и кооперация. В 2017 году индекс включил 193 страны, среди которых государства-члены ЧЭС заняли следующие места (в порядке возрастания угроз кибербезопасности): Грузия - 8, Россия – 10, Румыния -42, Турция - 43, Болгария - 44, Азербайджан - 48, Украина - 59, Греция - 64, Молдова - 73, Албания - 89, Сербия - 90, Армения - 111.

22. Государства-члены ЧЭС, также как и многие другие страны мира, предпринимают всеобъемлющие меры по борьбе с угрозами кибербезопасности 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 целый ряд мероприятий в научно-исследовательской сфере.

23. Необходимо объединить интересы и 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. Необходимо принять и укрепить соответствующее законодательство. Необходимо также создать сеть взаимодействия специалистов, представляющих все заинтересованные сектора, включая правительство, банки, энергетическую и транспортную промышленность, коммерческие объекты и телекоммуникации.

24. Согласно Указу Президента ***Азербайджанской Республики*** «О мерах по усовершенствованию деятельности в сфере информационной безопасности» от 26 сентября 2012-го года № 708, Министерству связи и информационных технологий Азербайджанской Республики было поручено регулярно анализировать общее состояние кибербезопасности в стране, осуществлять информирование населения, частных и других структур об электронных угрозах, существующих и способных возникнуть во время использования электронных средств, оказывать им техническую и методическую помощь, в целях предотвращения глобальных кибератак.

25. В целях координации деятельности субъектов информационной инфраструктуры в области кибербезопасности, информирования на уровне страны о существующих и способных возникнуть электронных угрозах, просвещения населения, частных и других структур в области кибербезопасности и оказания им методической помощи при Министерстве связи и информационных технологий Азербайджанской Республики создан Центр Электронной Безопасности, являющийся координационной структурой.

26. Центр в 2016 году был принят в члены организации «Альянс кибербезопасности для взаимного прогресса» (CAMP - Cybersecurity Alliance for Mutual Progress). С помощью этой организации и союзов, созданных с целью обеспечения безопасности в киберпространстве, членам оказывается необходимая методическая помощь по вопросам кибербезопасности, новых киберугрозах, кибератаках, и новых методах борьбы с ними.

27. С целью сотрудничества в сфере кибербезопасности между странами-членами ЧЭС предлагается: создание между организациями по кибербезопасности стран-членов ЧЭС онлайн платформы на нескольких языках, с целью осуществления обмена оперативной информацией о киберинцидентах, кибератаках и угрозах; проведение недели кибербезопасности в странах-членах ЧЭС по темам: безопасное использование

социальных сетей и защита личной информации; пути ограничения нежелательной рекламы (спам); программное обеспечение, блокирующее компьютеры и требующих выплаты (ransomware), и пути защиты от них; проведение семинаров в школах и университетах; повышение информированности населения; распространение буклетов; организация совместных тренингов с участием специалистов соответствующих ведомств стран-членов ЧЭС.

28. В качестве государства-члена Европейского союза ***Болгария*** принимает участие в разработке и согласовании политики и инструментов Союза для повышения общего уровня кибербезопасности. Болгария активно поддерживает предложение о создании нового Агентства Европейского союза по кибербезопасности и о введении новой общеевропейской системы сертификации для обеспечения использования только защищенной продукции. Данный «пакет кибербезопасности» инициирован эстонским председательством в ЕС и продолжает рассматриваться и в рамках болгарского председательства в 2018 г. Планируется организация в Болгарии конференции по кибервызовам, которая обсудит актуальные вопросы европейской кибербезопасности.

29. Стандарты кибербезопасности на национальном уровне, закреплены в Директиве Европейского союза по сетевой и информационной безопасности. В рамках болгарского законодательства сформирована межведомственная рабочая группа под руководством Государственного агентства «Электронное управление», целью которой является внедрение положений Директивы ЕС в проект Закона о кибербезопасности. В 2009 г. решением Совета министров Республики Болгарии создана должность Национального координатора по вопросам кибербезопасности.

30. В 2016 г. Совет министров Республики Болгария принял Национальную стратегию кибербезопасности «Устойчивая к кибератакам Болгария 2020», в которой предусмотрено повышение ответственности спецслужб Республики Болгарии для укрепления и развития национальной системы кибербезопасности и достижения открытого, безопасного и защищенного киберпространства. Борьба с киберугрозами состоит из трех фаз. Первая (2016 г.) – укрепление институционального потенциала в области киберзащиты путем создания Национальной координационно-организационной сети кибербезопасности (НКОСКС), которая объединяет службы безопасности и государственные структуры в области ИКТ, Министерство внутренних дел и обороны, Министерство транспорта, информационных технологий и связи, а также Государственное агентство «Электронное управление». Вторая фаза концентрируется на принятие неотложных мер, включая мониторинг информационно-коммуникационных систем и определение критических национальных инфраструктур. Следующая фаза предусматривает создание в Болгарии в 2018-2019 гг. системы адекватного реагирования на кибератаки. В 2020 г. планируется достижение общей киберустойчивости на национальном уровне и обеспечение эффективного взаимодействия на международном уровне в регионе, в ЕС и НАТО. Запланировано через четыре года стать лидером в регионе в области кибербезопасности.

31. Правительство ***Грузии***, после широкомасштабных кибератак на интернет-пространство страны в 2008 г., решительно поддержало работу по защите государственных ИТ-систем. Под руководством Совета национальной безопасности в 2013 г. была принята «Стратегия национальной кибербезопасности Грузии (2013-2015 гг.)» и соответствующий План действий. В 2016 г. Постоянная межведомственная комиссия по подготовке концептуальных документов национальной безопасности при Совете по управлению проблемами государственной безопасности и кризисами была разработана Стратегия кибербезопасности на 2017-2018 гг. и соответствующий План мероприятий.

Данная Стратегия ориентирована на дальнейшее развитие области кибербезопасности. Основное внимание в новой стратегии уделяется расширению исследований и анализа, подготовке новой законодательной базы, повышению уровня осведомленности населения, развитию образования, профессиональной подготовки и международному сотрудничеству в области кибербезопасности с целью содействия обмену информацией, снижению уязвимости, а также определению и разработки стратегий сдерживания враждебной или вредной деятельности в киберпространстве.

32. В 2012 г. был принят закон «Об информационной безопасности», который устанавливает рамки для принятия эффективных и действенных мер, направленных на обеспечение информационной безопасности. Этим законом было создано Бюро кибербезопасности, основной задачей которого является защита важнейших ИКТ-систем Министерства обороны Грузии. Незаконный доступ, вмешательство в работу ИКТ-систем, злонамеренное использование технологичных устройств криминализируются Уголовным кодексом страны. Закон о защите личных данных был принят парламентом в 2011 году и призван обеспечить защиту прав и свобод человека, в том числе права на неприкосновенность частной жизни в процессе обработки персональных данных, а также определяет полномочия и обязанности соответствующих ведомств в этом отношении. В соответствии с законом за обеспечение кибербезопасности в Грузии отвечают Агентство по обмену данными Министерства юстиции Грузии (CERT.GOV.GE) и Бюро кибербезопасности Министерства обороны Грузии. В 2012 г. в Министерстве внутренних дел был создан Департамент по борьбе с киберпреступностью, которая ведет расследования киберпреступлений. В департаменте круглосуточно работает Контактная группа, формированная на основе Конвенции Совета Европы о киберпреступности.

33. В 2013 г. в сотрудничестве с Бюро НАТО по связи (NLO) Рабочая группа министерства обороны с участием эстонского эксперта изучила проблематику кибербезопасности в системе обороны. В результате этой работы был подготовлен «план развития» (roadmap), который лег в основу создания Бюро кибербезопасности. В 2017 г. была создана оперативно-техническая служба, которая реагирует на кибератаки, направленные против безопасности страны. Бюро кибербезопасности активно сотрудничает в рамках НАТО как на двустороннем, так и многостороннем уровнях. Бюро участвует в двух проектах по линии «умной обороны» (smart defense) - многонациональной программе обмена информацией по вредной ПО (MN MISP) и многонациональной программе повышения уровня информированности о киберпреступлений (MN CD E&T).

34. В ***Греческой Республике*** Отдел киберпреступности является структурой полиции, которая занимается вопросами кибербезопасности и борьбы с киберпреступностью. Основными направлениями деятельности являются предотвращение и расследование преступлений, совершенных в Интернет-среде либо в рамках онлайн-действий. Этот Отдел состоит из пяти департаментов, охватывающих широкий спектр сфер: Департамент административной поддержки и обработки информации; Департамент стратегического управления инновационной деятельностью; Департамент электронных услуг, телефонной связи, безопасности программного обеспечения и защиты авторских прав; Департамент кибербезопасности для несовершеннолетних и цифровых расследований; Департамент по особым делам и расследованию электронных преступлений. Отдел киберпреступности успешно расследует киберпреступления.

35. Греция включила положения Конвенции Совета Европы о киберпреступности в национальное законодательство в области борьбы с электронной преступностью.

Греция активно осуществляет постоянный обмен криминальной информацией на основе двусторонних и многосторонних соглашений о сотрудничестве через институционализированные информационно-коммуникационные каналы. Более полно используются существующие инструменты и услуги в рамках Европейского центра киберпреступности Europol-EC3 и Интерпола. Ведется тесное сотрудничество с правительственными органами и учреждениями с целью обеспечения цифровой безопасности и защиты государственных инфраструктур.

36. Национальная группа по реагированию на чрезвычайные ситуации в киберпространстве (CERT) является органом по борьбе с кибератаками. Она контролирует появление электронных атак, анализирует их и обеспечивает информационную безопасность баз данных. Для большей эффективности группа сотрудничает с иностранными структурами CERT, а также с государственными службами внутри страны. Центр по изучению проблем безопасности Министерства внутренних дел в сотрудничестве с Фондом исследований и технологий «FORTH», Университетом им. Аристотеля в Салониках и Греческим саморегулируемым органом по обеспечению безопасности Интернет-контента «Safenet» в рамках программы ЕС Генерального директората по внутренним вопросам создал Греческий центр киберпреступности (GCC). Этот центр является частью нового механизма скоординированных усилий на уровне ЕС для повышения уровня информированности о киберпреступлениях.

37. Правительство ***Республики Молдова*** постановлением № 857 от 31.10.2013 утвердило Национальную стратегию развития информационного общества «Moldova digitală 2020» (Цифровая Молдова 2020) и План действий по ее внедрению, разработанные Министерством информационных технологий и связи. Национальная программа по кибербезопасности Республики Молдова 2016-2020 гг. была утверждена Постановлением Правительства № 811 от 29.10.2015 г. Эти документы создают основу кибербезопасности и устанавливают цели обеспечения информационной безопасности. Для реализации этих целей принято решение правительства о минимальных обязательных требованиях в отношении информационных систем и уже существующих информационных ресурсов для обеспечения адекватного уровня защиты информационных систем (Постановление Правительства № 201 от 28.03.2017 г.).

38. Высший совет безопасности в своем Решении № 01 / 1-02-05 от 07.10.2014 г. подтверждает, что обеспечение информационной безопасности является основным элементом в обеспечении национальной безопасности, который содействует построению информационного общества в Республике Молдова, основанного на доверии граждан к информационным технологиям и электронным коммуникациям. В соответствии с Постановлением Правительства № 746 от 18.08.2010 г. «Об утверждении обновленного Индивидуального плана действий по партнерству Республики Молдова – НАТО» в рамках Центра специальных телекоммуникаций создан Центр по обеспечению кибернетической безопасности (CERT-GOV-MD).

39. В полномочия CERT-GOV-MD входит обеспечение информационной безопасности государственных учреждений в киберпространстве, посредством сбора и анализа информации о кибератаках, а также принятия срочных и эффективных мер по защите информационных ресурсов органов публичного управления. Центр принимает и обрабатывает информацию по компьютерным инцидентам, которые имеют или могут иметь место в отношении национальных пользователей информационных систем и сети Интернет, представляет рекомендации по применению средств защиты

информации от компьютерных угроз, оказывает содействие пользователям и государственным органам Республики Молдова в расследовании компьютерных инцидентов, организовывает обучение и проведение тренингов по вопросам обеспечения информационной безопасности.

40. Республика Молдова продолжает принимать усилия по расширению институциональных возможностей в области кибербезопасности и защиты стратегических коммуникационных и информационных систем против кибератак и заинтересована в развитии сотрудничества с НАТО в области кибербезопасности и борьбе с современными угрозами безопасности.

41. ***Румыния*** активно принимает меры по укреплению кибербезопасности. В рамках Национальной стратегией кибербезопасности Национальная система кибербезопасности (NCSS) является общей схемой сотрудничества, объединяющей государственные специализированные органы и учреждения в этой области с целью координации национальных действий, которые обеспечивают безопасность киберпространства.

42. Национальная группа по реагированию на чрезвычайные ситуации в киберпространстве (CERT-RO) является независимым органом по предотвращению, обнаружению, идентификации инцидентов информационной безопасности, а также реагированию на них. Группа использует систему раннего оповещения на основе полученных данных и накопленной информации в области кибербезопасности. CERT-RO проводит информационные кампании, оказывает консалтинговые услуги и сотрудничает с другими органами в Румынии, Европейском союзе и за его пределами с тем, чтобы повысить уровень информации о кибер-угрозах и реагированию на инциденты. Работу CERT-RO, которая полностью финансируется из государственного бюджета, координирует Министерство связи и информационного общества.

43. На основе Директивы по безопасности сети и информационных систем (NIS), принятой Европейским парламентом в 2016 году, Министерство связи и информационного общества при поддержке CERT-RO разработало план транспонирования положений Директивы, который был опубликован и представлен на публичные консультации и в настоящее время находится в процессе одобрения. Этот план предусматривает в первую очередь укрепление институциональной структуры, создание механизма сотрудничества на национальном уровне и в сотрудничестве с европейскими партнерами для поддержки и выполнения стратегических целей обмена информацией.

44. В рамках Цифровой повестки дня для Европы 2020 Румыния определила четыре приоритетных направления: (1) электронное правительство, кибербезопасность, облачные вычисления, открытые данные, социальные медиа; (2) ИКТ в области образования, здравоохранения, культуры; (3) Электронная коммерция, исследования, разработки и инновации в области ИКТ; (4) Инфраструктура широкополосных и цифровых услуг.

45. В ***Республике Сербии*** действует Закон об информационной безопасности («Официальная газета Республики Сербии» № 6/16 и 94/17), который регулирует использование информационно-коммуникационных систем и обеспечение информационной безопасности. В рамках этого закона компетентным органом обеспечения информационной безопасности в Республике является Министерство торговли, туризма и телекоммуникаций. Закон также формирует национальный CERT - Агентство по регулированию в области электронных коммуникаций и почтовых услуг, а также CERT государственных органов - правительственное ведомство по

использованию информационных технологий и системы электронного правительства. Кроме того, Закон об организации и полномочиях государственных органов для борьбы с высокотехнологическими преступлениями («Официальная газета РС», № 61/05 и 104/09) определяет компетенцию специальных ведомств прокуратуры и Министерства внутренних дел, работающих в области высокотехнологичной преступности.

46. Правительство Республики Сербии утвердило Стратегию развития информационного общества в Республике Сербия на 2017-2020 гг. («Официальная газета РС», № 53/17). В Стратегии определены приоритетные направления развития информационной безопасности: 1) безопасность системы ИКТ; 2) информационная безопасность граждан; 3) борьба с высокотехнологичной преступностью; 4) обеспечение информационной безопасности Республики Сербии и 5) международное сотрудничество. Правительство РС сформировало Координационный орган по вопросам информационной безопасности, который состоит из представителей ведомств, работающих в области информационной безопасности. Координационный орган организует сотрудничество между соответствующими структурами в области повышения уровня информационной безопасности и проведения профилактических мероприятий, направленных на укрепление кибербезопасности.

47. Республика Сербия активно сотрудничает с другими государствами и международными организациями в области предупреждения высокотехнологичной преступности. Республика Сербия участвует в работе Международного союза электросвязи и Организации по безопасности и сотрудничеству в Европе (ОБСЕ). В этой связи предлагается расширить сотрудничество в области кибербезопасности между государствами-членами ПАЧЭС путем организации обмена информацией, знаниями и опытом национальных и международных центров кибербезопасности для предупреждения и предотвращения атак на информационные системы.

48. В ***Турции*** Стратегия кибербезопасности включает следующие основные направления: операции по киберзащите и киберсдерживанию; борьба с киберпреступностью; кризисное управление; управление сетью Интернет; координировать действия между соответствующими учреждениями. Основной целью правительства является интегрирование сферы кибербезопасности в систему национальной безопасности Турции.

49. Одним из наиболее важных шагов в отношении политики кибербезопасности стало решение Совета Министров, предпринятое в июне 2012 года № 3842 «О реализации, управлении и координации работы по обеспечению национальной кибербезопасности». В соответствии с этим решением, с целью подготовки политики, стратегии и плана действий в отношении кибербезопасности был сформирован Комитет по кибербезопасности (SGK). В стране за обеспечение кибербезопасности отвечает Министерство транспорта, судоходства и коммуникаций. В 2013 году решением Комитета по кибербезопасности был создан Национальный центр реагирования на киберинциденты (USOM).

50. «Национальная киберстратегия и План действий на 2013-2014» учитывает основные факторы, влияющие на политику турецкой национальной кибербезопасности, и выдвигает ряд целей. Среди них: принятие дополнительных законов в сфере кибербезопасности и усовершенствование имеющихся; создание команды реагирования на киберугрозы (SOME) под контролем USOM; разработка надежных механизмов записи для определения источника кибератаки и ее влияния; укрепление

безопасности общественных информационных систем и обеспечение новыми технологиями; подготовка людских ресурсов в области кибербезопасности и организация информационно-просветительских мероприятий, развитие местных технологий для обеспечения кибербезопасности и расширение сферы работ в учреждениях, ответственных за обеспечение национальной кибербезопасность.

51. Для более эффективной борьбы против киберугроз требуется активизировать двустороннее и многостороннее сотрудничество для наращивания потенциала и повышения уровня информированности в области кибербезопасности. Предлагается обратить внимание на следующие сферы в рамках сотрудничества между государствами-членами ЧЭС: обмен информацией о рамках национальной кибербезопасности; организация рабочих визитов; обмен экспертами; обмен разведывательной информацией о контругрозах; организация совместных учений в области кибербезопасности; организация совместных конференций и семинаров по тематике кибербезопасности.

52. В недавно принятом Законе ***Украины*** «Об основных принципах обеспечения кибербезопасности Украины» определяются основные правовые и организационные основы обеспечения защиты жизненно важных интересов человека, общества и государства, национальных интересов Украины в киберпространстве, основные цели, направления и принципы государственной политики в сфере кибербезопасности, полномочия государственных органов, предприятий, учреждений, организаций, лиц и граждан в этой сфере.

53. В рамках выполнения проекта Совета Европы и Европейского Союза «Киберпреступность и Восточное партнерство» готовится проект изменений в Уголовно-процессуальный кодекс Украины с целью надлежащей имплементации Конвенции о киберпреступности. Предлагается совершенствование процессуальных механизмов сбора доказательств в электронной форме и введение особого порядка снятия информации с каналов телекоммуникаций по решению суда, во время досудебного расследования преступлений. Предусмотрен порядок срочного фиксирования и хранения компьютерных данных. Также определен порядок блокировки определенного (идентифицированного) информационного ресурса (информационного сервиса). Ожидается, что этот законопроект также урегулирует взаимоотношения между правоохранительными органами и провайдерами, а также между правоохранительными органами и разведкой и контрразведкой.

54. Также проведен ряд рабочих встреч представителей Национальной полиции Украины, Службы безопасности Украины, Министерства юстиции, Национальной комиссии, осуществляющей государственное регулирование в сфере связи и информатизации, в ходе которых обсуждены предложения изменений в законодательство и высказаны замечания и предложения по их дальнейшему совершенствованию. Кроме того, проведено рабочее совещание с участием специалистов Ассоциации «Телекоммуникационная палата Украины». С целью принятия мер по ограничению участия каких-либо субъектов хозяйственной деятельности в мероприятиях по обеспечению информационной и кибербезопасности, в частности в усилении государственного контроля за состоянием криптографической и технической защиты информации по ограничению использования продукции, технологий и услуг таких субъектов, в Национальной полиции разработано поручение «Об организации мероприятий по реализации Стратегии кибербезопасности Украины».

55. Важными обязанностями в деле обеспечения кибербезопасности является подготовка всеобъемлющего национального плана по обеспечению ключевых ресурсов и ключевой инфраструктуры; 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 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 кибербезопасности.

56. Защита объектов киберпространства требует усилий многих стран и граждан. Технологии, создающие и поддерживающие киберпространство, стремительно развиваются а угрозы и уязвимость систем постоянно меняются. Необходимы координированные усилия для определения и исправления самых серьезных проблем уязвимости с помощью совместных действий, таких как обмен передовым опытом, оценка и использование новейших технологий.

57. Экономика и национальная безопасность становятся все более зависимы от информационных технологий и информационной инфраструктуры. Глобальное киберпространство поддерживает деятельность всех секторов экономики: энергетику (электроэнергия, нефть и газ), перевозки (железнодорожные, воздушные, морские), финансы и банковское дело, информацию и телекоммуникации, здравоохранение, службы экстренной помощи населению, водоснабжение, химическое производство, оборону, промышленность, пищевую промышленность, сельское хозяйство и почтовые услуги. Поэтому кибератаки на информационные сети могут привезти к серьёзным последствиям для ключевой деятельности.

Международное сотрудничество

58. Одним из главных инструментов укрепления международной кибербезопасности является Конвенция Совета Европы о киберпреступности (2001 г.), которая вступила в силу в 2004 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, включая экстрадицию 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. Конвенция дополняется Протоколом об уголовной ответственности за акты ксенофобии и расизма, совершенные при помощи компьютерных систем, который вступил в силу 1 марта 2006 года *(все государства-*

члены ЧЭС подписали и ратифицировали Конвенцию кроме России; все государства-члены ЧЭС подписали и ратифицировали Протокол кроме Азербайджана, Болгарии, Грузии, России; Турция подписала, но не ратифицировала Протокол).

59. 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. Одним из базовых инструментов обеспечения международной информационной безопасности являются меры укрепления доверия, принятые в рамках ОБСЕ. Меры доверия нацелены на снижение рисков возникновения конфликтов при использовании информационных и коммуникационных технологий. В Организации работает неформальная рабочая группа, которая создана в соответствии с решением № 1039 Постоянного совета ОБСЕ от 2012 г. В 2016 г. принято решение № 1202 «меры укрепления доверия в рамках ОБСЕ с целью сокращения рисков возникновения конфликтов в результате использования информационных и коммуникационных технологий».

60. Глобальные вопросы кибербезопасности, которые затрагивают интересы практически всех стран мира, обсуждаются под эгидой Организации Объединенных Наций. Генеральная Ассамблея ООН приняла резолюции по кибербезопасности. 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. Придавая важное значение международной информационной безопасности как одному из ключевых элементов системы международной безопасности, в рамках ООН ведется работа по разработке Конвенции по вопросам кибербезопасности.

61. НАТО разработала свою первую политику в области кибероборонь в 2007 г., которая служит основой для других стратегических документов и деятельности в этой области. НАТО была 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 кибероборонь, принятая в 2007 г., создала первоначальные механизмы для консультаций с государствами-членами по вопросам кибероборонь. В стратегической концепции НАТО, принятой на Лиссабонском саммите в ноябре 2010 г., подчеркивается, что НАТО должна ускорить принятие мер в ответ на угрозу кибератак. На Лиссабонском саммите была подготовлена «дорожная карта», которая 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 2017 г. Таллинне (Эстония) основали Объединенный центр передовых технологий по кибероборонe НАТО (NATO Cooperative Cyber Defence Centre of Excellence), который сегодня является флагманом европейской кибербезопасности. Центр ежегодно

проводит крупнейшие в мире киберучения Locked Shields для экспертов в области киберзащиты. Усилиями центра разрабатывается доктрина по киберзащите - единый алгоритм действий, которому будут следовать страны в случае нападения. Ожидается, что новая доктрина будет одобрена НАТО в 2019 году. НАТО и ЕС одновременно проводят скоординированные учения, чтобы испытать свою способность реагировать на современные киберугрозы.

62. Цифровая повестка дня для Евросоюза (DAE) была запущена Европейской Комиссией в мае 2010 г. в целях поддержки экономического роста в Европе и предоставления помощи гражданам и предприятиям Европы, для получения максимальной отдачи от цифровых технологий. В 2013 году в Европейском Союзе была сформулирована и одобрена стратегия Кибербезопасности. Целью стратегии кибербезопасности ЕС (Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace) является повышение устойчивости и наращивание потенциала в области кибербезопасности государств-членов ЕС (усиление борьбы с киберпреступностью, формирование эффективной инфраструктуры обеспечения безопасности, разработка принципов международной политики в области кибербезопасности). В 2017 г. было принято решение сделать существующую стратегию более современной, чтобы она принимала во внимание все новые задачи и технологии. Еврокомиссия предложила ряд мер по усилению кибербезопасности, среди которых – создание Агентства ЕС по кибербезопасности. Агентство будет создано на основе существующего Европейского агентства по сетевой и информационной безопасности (ENISA), которое будет помогать странам ЕС в борьбе с кибератаками. Ключевым инструментом для защиты информационных инфраструктур критической значимости является Компьютерная программа быстрого реагирования «CERT» (Computer Emergency Response Teams). Данные команды существуют в государствах ЕС и призваны быть основным поставщиками услуг безопасности для государства и граждан, а также заниматься просветительской деятельностью. Государства-члены со своей стороны должны гарантировать, что у них имеется необходимый уровень национальных возможностей и средств для обеспечения кибербезопасности.

III. ВЫВОДЫ

63. За последние несколько лет резко возросли угрозы безопасности киберпространства. Учитывая возрастающую зависимость от киберпространства практически в каждой сфере жизни, страны и международные организации активно укрепляют политику по защите информационных систем и обеспечению противодействия киберугрозам.

64. Надёжность и безопасность киберпространства имеет огромное значение для государств и общества. Инфраструктура, с помощью которой создается киберпространство носит глобальный характер. В киберпространстве национальные границы не имеют значения. В силу глобального характера киберпространства, имеющиеся уязвимости распространяются на весь мир и доступны для каждого, кто захочет злоупотреблять ими. Обеспечение кибербезопасности в настоящее время является главным вызовом для государств как на национальном, так и международном уровне.

65. Каждая страна должна инвестировать в необходимые навыки и образование для того, чтобы люди могли работать в сфере информационной безопасности, а также обеспечивать сотрудничество между государственным, частным и научным секторами. Использование программ по борьбе с угрозами кибербезопасности и снижению уровня уязвимости, а также рост осведомленности о безопасности киберпространства и

повышение профессиональной подготовки являются велением времени. Следует стимулировать, пропагандировать, развивать и решительно внедрять глобальную культуру кибербезопасности.

66. Законы и правила, касающиеся кибербезопасности, необходимо принимать и постоянно обновлять, поскольку одного лишь принятия и осуществления национальных законов недостаточно для решения современных проблем кибербезопасности. 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.

67. Во взаимосвязанном мире с наличием мириад устройств, включая компьютеры, смартфоны, планшеты, все пользуются одним и тем же каналом связи, и каждый пользователь играет свою роль в обеспечении безопасности своего и общего киберпространства. Защита Интернета и других цифровых ресурсов является общей ответственностью. Необходимо помнить о том, что кибербезопасность начинается с ответственного поведения в киберпространстве каждого отдельного пользователя.

68. Очень важно принимать усилия для укрепления кибербезопасности, улучшать координацию реагирования на кибератаки, содействовать установлению партнерских отношений по защите информационной инфраструктуры и способствовать созданию национальных и международных систем наблюдения и предупреждения кибератак по мере их появления. Уязвимость в киберпространстве является реальной, серьезной и быстро разрастающейся проблемой.

69. Сегодня глобальная информатизация является ключевой тенденцией развития общества. В этих условиях безопасность в сфере использования информационных и коммуникационных технологий становится одним из основных вопросов международной повестки дня. Вопросы кибербезопасности консолидируют мировое сообщество и с помощью укрепления всеобщего понимания реальной опасности киберугроз формирует повестку дня, направленную на создание действительно надежной и защищенной информационной среды.