# II

# СЕКЦИЯ

# Укрепление международной безопасности: роль парламентов

СЕКЦИЯ II

# Укрепление международной безопасности: роль парламентов

В современном мире продолжает обостряться комплекс проблем международной и национальной безопасности, укрупняется масштаб новых вызовов и угроз.

К наиболее серьезным, фундаментальным угрозам глобального характера следует отнести систематическое игнорирование группой стран основополагающих норм международного права, тенденцию к односторонним подходам, применению методов силового или санкционного давления на суверенные государства, вмешательства в их внутренние дела.

К системным рискам для международной безопасности на современном этапе относится эскалация напряженности и рост конфликтного потенциала, усиление конфронтации в различных регионах мира, конвенциализация опоры на силовой фактор, распространение блоковых подходов и игры с «нулевой суммой» вместо устойчивых коллективных решений на основе компромисса и взаимного учета интересов.

Как отметил Президент России В. В. Путин, «за последнюю четверть века порог применения силы уже явно снизился... Приобретенный после двух мировых войн антивоенный иммунитет, который существовал на психологическом, подсознательном уровне, стал ослабевать».

Серьезными угрозами глобального уровня, прямо влияющими на безопасность большинства стран и целых регионов, остаются международный терроризм, наркотрафик, распространение ядерного оружия, а также угрозы международной информационной безопасности.

На новом этапе технологического развития вооружений и военной техники в условиях роста международной напряженности, особую актуальность приобретают вопросы современного состояния системы контроля над вооружениями, а также нераспространения оружия массового уничтожения (ОМУ) и средств его доставки.

В этом контексте возрастает роль парламентов не только как ключевых разработчиков правового регулирования в сфере безопасности и драйверов его международной гармонизации, но и в качестве авторитетных проводников утверждения коллективных начал в мировых делах и объединительной повестки противодействия традиционным и новым вызовам и угрозам, деэскалации напряженности в международных отношениях, снижения конфронтации и конфликтного потенциала, широкого сотрудничества между государствами и их объединениями в интересах обеспечения международной и региональной безопасности и стабильности, в том числе по линиям Восток – Запад и Север – Юг, устранения возникающих угроз миру, урегулирования разногласий на основе равноправного взаимоуважительного диалога при неукоснительном соблюдении основополагающих норм международного права в интересах безопасности и благополучия народов, утверждения принципов ответственного поведения в мировом информационном пространстве, отказа от односторонних попыток решения международных споров с применением силы или санкционного давления.

## 1. Международный терроризм как глобальная угроза

У понятия *«международный терроризм»* (МТ) нет единой общепризнанной трактовки. Вместе с тем разработано достаточное количество документов ООН, нормативных актов и рекомендаций по самым разным аспектам борьбы с терроризмом.

Международный терроризм имеет присущие только ему особенности, которые отличают его от других разновидностей террористической деятельности. К МТ причисляются террористические акции, осуществляемые на территории двух и более государств либо затрагивающие интересы двух и более государств, а также скоординированная деятельность террористических организаций (ТО) в нескольких странах.

### 1.1. Современный терроризм: ключевые характеристики

*Активизация МТ* тесно связана с распространением религиозно-идеологического экстремизма в странах Ближнего и Среднего Востока, которое усилилось после падения светских авторитарных режимов («арабский социализм» в Египте, Сирии, Ираке).

Радикальный исламизм[1] во многих мусульманских странах является ответной реакцией на процессы *глобализации, растущее вмешательство США и других западных стран во внутренние и региональные процессы в странах Ближнего и Среднего Востока, неурегулированность внутренних социальных и политических проблем в этих странах.*

Рост международной террористической активности сопровождает обострение конкуренции за политическое и экономическое лидерство и контроль над мировой финансовой системой и природными ресурсами (включая нефтедобычу) между ключевыми мировыми державами на фоне глобализации и перехода к новому экономическому укладу.

Международные террористические группы, получая в ряде случаев внешнюю поддержку, используют ее для реализации собственных стратегий и расширения своего влияния.

Опора на внешнюю финансовую и материально-техническую поддержку и новые ИКТ-технологии (соцсети, зашифрованные мессенджеры, интернет-банкинг, криптовалюты) позволили международному терроризму *масштабироваться от преимущественно регионального явления (локальные террористические группы) до уровня глобальной угрозы* (международные сетевые структуры). При этом, однако, и локальные террористические группировки (как, например, ХАМАС) во многом сохраняют свою роль и влияние в соответствующих регионах, но уже не определяют лицо современного терроризма.

[1] Радикальный исламизм представляет собой религиозно-политическую оппозицию существующим политическим режимам в мусульманских странах и выступает за полное переустройство общества и государства в соответствии с нормами шариата. Он составляет основное ядро идеологии исламистских ТО.

*Рисунок 1*

**Число жертв террористических группировок, 2000–2016 гг.**

***Источник:*** *Global Terrorism Index / Institute for Economics and Peace, 2017, p. 72 (https://reliefweb.int/sites/reliefweb.int/files/resources/Global%20Terrorism%20Index%202017%20%284%29.pdf).*

Феномены «Аль-Каиды» и «Исламского государства» (ИГ) как террористических структур нового типа связаны с использованием современных сетевых и медиатехнологий, которые ими используются как для пропаганды и вербовки сторонников, так и для поиска новых источников финансирования.

Глобализация террористических сетей привела к их тесному сращиванию с международным оборотом криминальных денег. В результате образовались международные «транснациональные криминальные корпорации» с собственной нелегальной хозяйственно-экономической активностью. Террористы играют в них роль силового крыла[2]. Использование новых организационных форм и сетевых технологий привело к значительному росту террористической активности этих структур и пропорциональному увеличению экономического ущерба от их деятельности (рис. 1 и 2).

Оценка численности ключевых террористических группировок в мире, включая ИГ и «Аль-Каиду», приведена в таблице 1.

Основные регионы систематической активности террористов фактически не меняются в течение последних нескольких лет. Ключевыми из них являются:

1) Сирия и Ирак, где действуют ИГ, «Хезболла» и «Джейш аль-Фаттах», в которую в 2015 году вошла группировка «Джабхат ан-Нусра»;

2) Афганистан и Пакистан, где велико влияние «Талибана» и где пытается укрепиться ИГ;

3) Нигерия («Боко Харам» в координации с ИГ);

4) Йемен («Аль-Каида на Аравийском полуострове»);

5) территории бывшего единого Сомали («Аш-Шабаб» и другие группировки);

6) страны Западной Африки (активны «Боко Харам», группы бывшей «Аль-Каиды в Магрибе» и «Ансарад-Дин»);

7) государства Магриба и Египет («Братья-мусульмане», усиливается также давление со стороны террористических сетей, базирующихся в соседних регионах).

Кризисные развивающиеся страны, отягощенные этническими и религиозными конфликтами, чьи центральные правительства ослаблены, а возможности спецслужб и силовых структур ограничены, используются террористами в качестве баз-убежищ и зон перегруппировки.

Международные террористические группировки осуществляют целенаправленное проникновение в развитые страны в целях вербовки сторонников и бойцов, поиска новых источников финансирования (в основном пожертвования). Силами сформированных «на местах» террористических ячеек им также удается осуществлять резонансные и жестокие теракты против мирного населения (в Мадриде в 2004 году – 192 жертвы, Лондоне в 2005 году – 52 жертвы, Париже в 2015 году – 130 жертв, в аэропорту и метро Брюсселя в 2016 году – 33 жертвы, взрывы в метро Санкт-Петербурга в 2017 году – 15 жертв, и другие).

**Таблица 1.** Численность основных террористических группировок

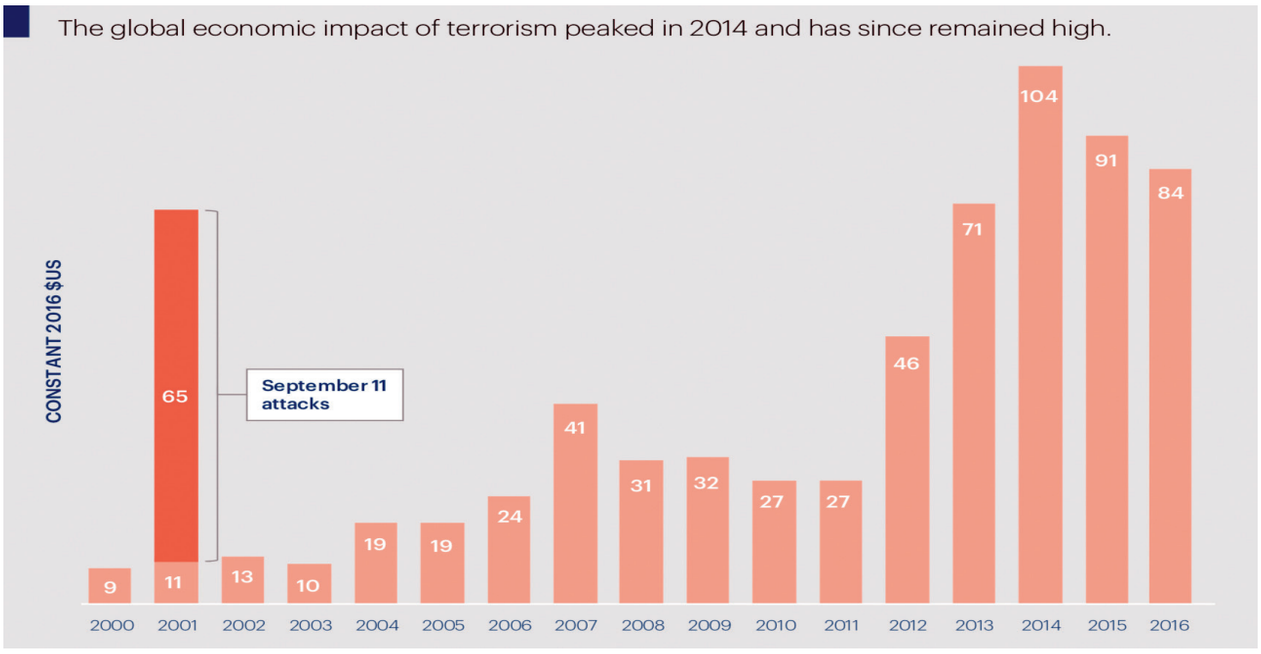
| Организация | | Оценка численности активных бойцов на 2016-2017 гг., тыс. чел. |
|---|---|---|
| «Исламское государство» | в Сирии и Ираке | 12–15 |
| | в Ливии | до 6 |
| «Аль-Каида» | на Аравийском п-ве | до 4 |
| | в Магрибе | несколько |
| «Талибан» | в Афганистане | до 60 |
| | в Пакистане | несколько |
| «Джабхат ан-Нусра» | | до 10 |
| «Аш-Шабаб» | | до 5 |
| «Боко Харам» | | 7–10 |

***Источники:*** *Country Reports on Terrorism / U.S. Department of State, 2017; Giustozzi A. Afghanistan: Taliban's organization and structure / Landinfo, 2017.*

[2] Hesterman J. Transnational Crime and the Criminal-Terrorist Nexus: Synergies and Corporate Trends. Maxwell, AB: AirUniversity, 2004. P. 62–65.

*Рисунок 2*

**Экономические последствия терроризма, 2000–2016 гг., млрд долл.**




***Источник:*** *Global Terrorism Index / Institute for Economics and Peace, 2017, p. 80 (https://reliefweb.int/sites/reliefweb.int/files/resources/Global%20Terrorism%20Index%202017%20%284%29.pdf).*

## 1.2. Источники и объемы финансирования терроризма

Почти у всех группировок заметную часть доходов составляют *сборы пожертвований и/или прямые поборы. Наиболее организационно развитые квазигосударственные террористические группировки активно монетизируют ресурсы* подконтрольных территорий (табл. 2).

Для «Исламского государства» в 2014–2016 годах основным источником доходов являлась реализация нефти и продуктов ее переработки с подконтрольных в то время месторождений в восточной Сирии. Для «Талибана» важнейшим каналом финансирования является афганский героиновый наркотрафик. Для ряда латиноамериканских группировок -кокаиновый наркотрафик.

Регистрируется широкое применение террористами нерегулируемых финансовых инструментов, в первую очередь криптовалют[3]. Финансовая база террористов растет за счет глобализации и диверсификации сети пожертвований и повышения надежности системы платежей.

**Таблица 2.** Оценка годового дохода некоторых крупных террористических групп в 2016 г.

| Организация | Годовой объем доходов, млн долл. |
|---|---|
| «Исламское государство» | 2000 |
| «Талибан» | 400 |
| «Аль-Каида» (все ветви) | 250 |
| «Боко Харам» | 25 |

***Источник:*** *Global Terrorism Index 2017 / Institute for Economic and Peace, 2017.*

[3] Ward A. Bitcoin and the Dark Web: The New Terrorist Threat? // RAND Corporation, Jan 2018 (https://www.rand.org/blog/2018/01/bitcoin-and-the-dark-web-the-new-terrorist-threat.html).

## 1.3. Катастрофический терроризм

К текущему моменту в мире не были зафиксированы прецеденты так называемого катастрофического терроризма с применением оружия массового уничтожения и, в частности, с использованием ядерного оружия. Однако реализация подобных сценариев - не фантастика.

Экспертами рассматриваются следующие вероятностные сценарии осуществления актов катастрофического терроризма:

1) подрыв (возможно, с захватом) объекта гражданской ядерной инфраструктуры - АЭС;

2) загрязнение окружающей среды радиоактивными материалами;

3) получение террористами компонентов химического или бактериологического оружия;

4) создание так называемой гаражной бомбы: монтажа ядерного взрывного устройства из отдельных компонентов в крупном мегаполисе;

5) похищение ядерного боезаряда и теракт с его применением.

Ликвидированные в марте 2016 года в Бельгии террористы, как выяснилось, готовили теракт именно на атомной электростанции. В мире насчитываются сотни работающих гражданских атомных реакторов[4], что обуславливает высокую потенциальную опасность подобных терактов, разрушительная сила которых может быть критической как для государств, так и для целых регионов мира.

Ключевыми средствами профилактики и предотвращения таких опасных атак являются:

1) фокусное внимание и контроль со стороны компетентных международных организаций;

2) проработанность национального законодательства и регламентов;

3) детальная проработка обеспечения физической защиты при различных сценариях угроз;

4) высокая ответственность на национальном и местном уровнях за обеспечение физической защиты ядерных объектов;

5) развитие всеобъемлющего сотрудничества заинтересованных стран в сфере совершенствования физической защиты ядерных объектов, включающее совершенствование законодательства, обмен лучшими технологическими практиками, обмен данными спецслужб, взаимопомощь.

### 1.4. Роль ООН в борьбе с международным терроризмом

ООН последовательно принимала рамочные решения, касающиеся активизации и координации усилий по борьбе с терроризмом на международном уровне. Основное внимание в них уделялось развитию межгосударственных связей (дву- и многосторонних), созданию эффективных режимов розыска и судебного преследования, а также борьбе с финансированием террористической деятельности.

Современный корпус решений восходит к следующим базовым документам:

- Декларация о мерах по ликвидации международного терроризма (1994 год), дополненная резолюцией 51-й сессии ГА ООН (1997 год);
- Международная конвенция о борьбе с финансированием терроризма (1999 год);
- Глобальная контртеррористическая стратегия ООН (2006 год), согласовавшая общие подходы к борьбе с терроризмом и ликвидации условий, способствующих его возникновению.

Достаточно сложной проблемой на международном уровне является несовпадение перечней организаций, признаваемых террористическими в разных странах мира. Это вызвано разными факторами, от технических бюрократических сложностей в коллективной идентификации и учете образующихся, сливающихся, раскалывающихся и исчезающих группировок до политических причин.

ООН играет ключевую роль в согласовании списков террористических организаций. С 2017 года в системе ООН действует Контртеррористическое управление. Эта структура обладает потенциалом и полномочиями для выработки совместных решений в области борьбы с терроризмом, включая гармонизацию списков ТО и реализацию специальных программ. Тем не менее на площадке ООН пока не удается выработать универсальный перечень критериев для признания организации террористической.

Актуальная практическая задача – совершенствование единой международной системы розыска и судебного преследования террористов. Для этого требуется стыковка законодательства национальных государств в сфере борьбы с финансированием терроризма, а также согласованность регулирования трансграничных потоков миграции. Решение этих задач требует систематических межгосударственных контактов на парламентском уровне с целью обмена лучшими практиками и выработки общих подходов.

[4] В настоящее время в европейских странах насчитывается 150 атомных энергоблоков, в России – 37, в США – 99, в Азии – 137. См.: WorldNuclear GenerationandCapacity / NuclearEnergyInstitute, 2017. (https://www.nei.org/resources/statistics/world-nuclear-generation-and-capacity).

## 2. Борьба с наркоугрозой

### Рост оборота наркотиков – критическая угроза для человечества.

Ситуация с наркотиками в мире продолжает ухудшаться. Несмотря на международные усилия, глобальное производство наркотических средств, а значит, и их потребление продолжают нарастать. Все более ухищренными становятся производственные и сбытовые цепочки, транспортные и финансовые сети наркотрафика.

Трансграничный характер основных наркопотоков способствует увеличению числа наркозависимых во всем мире, особенно в среде молодежи. По данным ООН, **ежегодно от последствий употребления наркотиков в мире гибнет более 190 тысяч человек. В душевом пересчете это означает, что ежегодно человечество утрачивает порядка 28 миллионов лет здоровой жизни.**

Торговля наркотиками является одним из наиболее прибыльных и масштабных видов транснациональной преступности, **объем годового оборота** которого по разным оценкам составляет **от 400 до 650 млрд долл** (см. табл. 3). Значительная часть мирового незаконного оборота наркотиков приходится на кокаин и опиаты, ключевыми поставщиками которых на мировые рынки являются, соответственно, Колумбия и Афганистан.

**Наркотрафик системно связан с другими видами транснациональной преступности. Генерируемые им сверхприбыли формируют обширную финансовую базу для международного терроризма** и радикальных течений, **поддерживают коррупцию** и провоцируют **финансовые махинации по отмыванию денег,** трансформируются в **оборотные средства для незаконной торговли оружием и преступлений в киберпространстве, торговли людьми и организации нелегальной миграции.**

**Drugs and organized crime**

Source: UNODC, adapted from Europol, *SOCTA 2017*.

**В результате сращивания новых вызовов и угроз формируется глобальная криминальная антисистема, одной из несущих опор которой является наркотрафик.**

**Таблица 3.** Оценка годового оборота мирового черного рынка наркотических средств, млрд долл.

| Наркотик | Нижняя оценка объема продаж | Верхняя оценка объема продаж |
|---|---|---|
| Марихуана | 183 | 287 |
| Кокаин | 94 | 143 |
| Опиаты | 75 | 132 |
| Амфетамины и новые синтетические наркотики | 74 | 90 |

***Источник:*** *May C. Transnational Crime and the Developing World. Washington, DC: Global Financial Integrity, 2017. P. 4.*

Добиться сокращения объема наркотиков, попадающих на мировой рынок, можно за счет **вовлечения в системное взаимодействие всех стран и объединений, на территории которых базируются** те или иные **звенья цепочки наркотрафика** – от производства наркотических веществ до их конечного сбыта.

**Эффективные стратегии противодействия наркотрафику должны носить комплексный, инклюзивный характер и обеспечивать согласованное применение триады антинаркотических мероприятий:**

- пресечение производства;
- противодействие транзиту (изъятие наркотиков из оборота на этапе транспортировки, в том числе за счет пограничного контроля);
- сокращение и профилактика спроса в странах сбыта.

**Основой международного режима по контролю за распространением наркотиков являются три базовые антинаркотические конвенции ООН:**

- Единая конвенция о наркотических средствах (1961 год);
- Конвенция о психотропных веществах (1971 год);
- Конвенция о борьбе против незаконного оборота наркотических средств и психотропных веществ (1988 год).

Усилия Российской Федерации по борьбе с международной наркоугрозой фокусируются прежде всего на противодействии наркотрафику из Афганистана. Россия выступает за ужесточение, большую последовательность и скоординированность мер противодействия афганскому наркотрафику – активизацию операций по перехвату наркотиков и ликвидации нарколабораторий совместными усилиями властей Афганистана и ведомой США миссии НАТО «Решительная поддержка». Однако российские предложения об интеграции и интенсификации усилий в борьбе с афганской наркоугрозой, в том числе об организации совместных действий стран НАТО и ОДКБ, не поддерживаются США и Североатлантическим альянсом, несмотря на отдельные эпизоды взаимодействия на двусторонней основе.

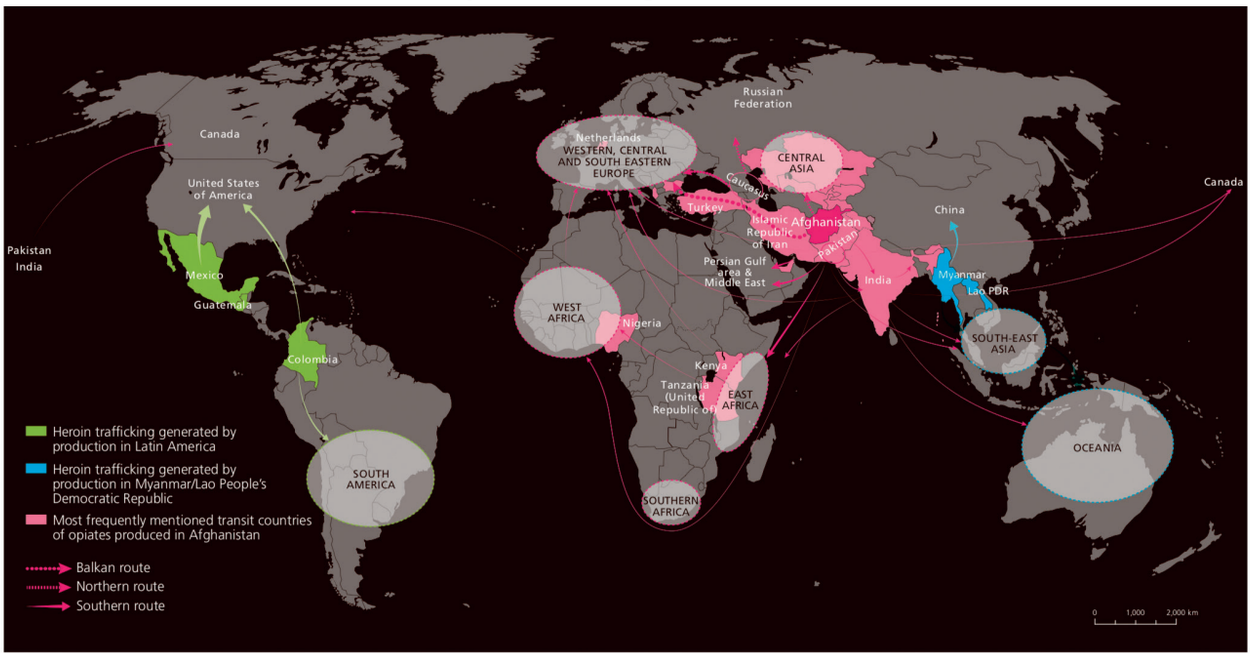
**При этом за период миссии Международных сил содействия безопасности (2001-2014 годы),** когда страна фактически находилась **под военным контролем ведомого США международного контингента, производство героина там не только не сократилось, но возросло в 40 раз и достигло 95 % от мирового.**

Контролируемая международными силами страна превратилась в мирового «опиумного монополиста». **Ежегодно в страны Европейского союза оттуда поступает 711 тонн опиума, в Россию – 549 тонн.**

Отсутствие реальных достижений в искоренении афганского наркотрафика оказывает глубокий пагубный эффект, подрывая авторитет институтов глобального управления и доверие народов к усилиям международного сообщества.

Интенсивная системная работа по противодействию афганской наркоугрозе ведется в рамках Организации

**Main opiate trafficking flows, 2011-2015**



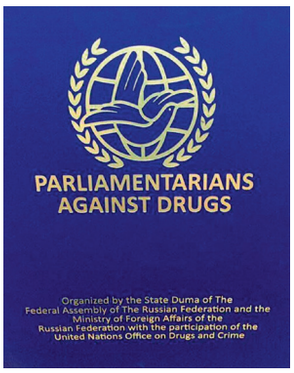

Sources: UNODC elaboration, based on responses to annual report questionnaire and individual drug seizure database.

*Notes: The trafficking flows are determined on the basis of country of origin/departure, transit and destination of seized drugs as reported by Member States in the annual report questionnaire and individual drug seizure database: as such, they are to be considered as broadly indicative of existing trafficking routes while several secondary flows may not be reflected. Flow arrows represent the direction of trafficking: origins of the arrows indicate either the area of manufacture or the one of last provenance, end points of arrows indicate either the area of consumption or the one of next destination of trafficking. The boundaries shown on this map do not imply official endorsement or acceptance by the United Nations. Dashed lines represent undetermined boundaries. The dotted line represents approximately the Line of Control in Jammu and Kashmir agreed upon by India and Pakistan. The final status of Jammu and Kashmir has not yet been agreed upon by the parties. The final boundary between the Sudan and South Sudan has not yet been determined. A dispute exists between the Governments of Argentina and the United Kingdom of Great Britain and Northern Ireland concerning sovereignty over the Falkland Islands (Malvinas).*

договора о коллективной безопасности (ОДКБ) и Шанхайской организации сотрудничества (ШОС).

ШОС с 2002 года формирует пояс безопасности для блокирования афганского наркотранзита. В ОДКБ[5] функционирует Координационный совет руководителей компетентных органов по противодействию незаконному обороту наркотиков.

**Законодательное обеспечение комплексной работы по противодействию распространению наркотиков - приоритет национальных парламентов и важнейшее направление межпарламентского сотрудничества.**




В декабре 2017 года в Москве по инициативе Государственной Думы состоялась **международная конференция «Парламентарии против наркотиков»**, собравшая представителей более чем 40 государств, руководителей законодательных и исполнительных органов власти, Управления ООН по наркотикам и преступности, ведущих профильных некоммерческих организаций.

Предметно рассматривались практические вопросы взаимодействия парламентариев разных стран в борьбе с наркоугрозой в контексте полномочий законодательной власти.

### Основные выводы дискуссий в ходе конференции:

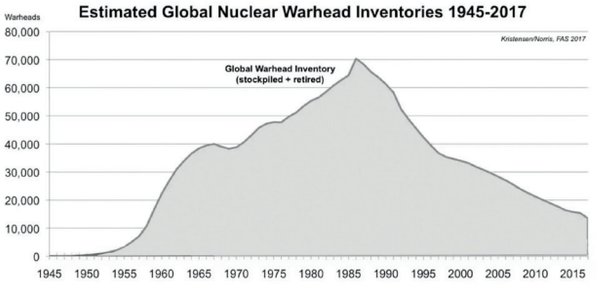
- **необходимость оперативного совершенствования правового регулирования и взаимной гармонизации национальных законодательств через обмен лучшими практиками;**
- **содействие парламентов в создании условий для интенсификации сотрудничества по линии национальных антинаркотических ведомств и правоохранителей;**
- **активизация законодательной и политической работы против пропаганды наркотиков, на ужесточение ответственности, на формирование в обществе устойчивого неприятия употребления наркотиков и пропагандирующей наркопотребление субкультуры;**
- **фокусировка мирового парламентского движения на противодействии наркоугрозе как одной из ключевых проблем безопасности - выдвижения антинаркотической тематики в число приоритетов международного парламентского сотрудничества в рамках различных двусторонних и многосторонних форматов, обеспечение системности работы на этом направлении;**
- **выстраивание в интересах достижения мира, свободного от наркотиков, инклюзивной системы взаимодействия законодательной и исполнительной власти, научно-экспертного сообщества, структур гражданского общества, институтов глобального управления, а также многосторонних межгосударственных объединений.**

[5] Государства – члены ОДКБ: Россия, Армения, Белоруссия, Казахстан, Киргизстан, Таджикистан.

## 3. Ядерное нераспространение и контроль над вооружениями

Краеугольным камнем системы международной безопасности являются режим нераспространения ядерного оружия (ЯО) и ядерное разоружение. Ядерное разоружение предполагает сокращение вплоть до ликвидации ядерных вооружений. В основе концепции нераспространения лежит предотвращение *горизонтального* распространения ЯО между странами, а также недопущение *вертикального* распространения, т. е. накапливания ЯО у ядерных держав.

**Рисунок 3.** Мировой ядерный арсенал по числу боеголовок, 1945-2017 гг.




***Источник:*** *Status of World Nuclear Forces / Federation of American Scientists, March 2018 (https://fas.org/issues/nuclear-weapons/status-world-nuclear-forces/).*

*После окончания холодной войны благодаря комплексу мер контроля над вооружениями и разоружению запасы ЯО удалось сократить.* В общей сложности мировой ядерный арсенал сократился *с 70 300 единиц*, которых он достигал *на пике холодной войны (1986 год), до 14 200 единиц по состоянию на 2018 год* (рис. 3).

### 3.1. Эрозия режима нераспространения ядерного оружия

Важнейшим инструментом, направленным на ограничение круга стран - обладателей ЯО, является **Договор о нераспространении ядерного оружия** (ДНЯО) 1967 года. Его участниками является 191 страна мира, а к числу ядерных держав отнесены Россия, США, Великобритания, Франция и Китай.

*В основу ДНЯО положен баланс трех составляющих: ядерного нераспространения, разоружения и соблюдения прав на использование атомной энергии в мирных целях.* Договор исключает передачу ЯО, а также материалов и технологий для его производства неядерным государствам. Вводятся международные гарантии для исключения перевода мирного использования атомной энергии в военное русло. *Особое место в Договоре занимает статья VI, прямо связывающая участников обязательствами по дальнейшему ядерному разоружению.*

*Каждые пять лет проводится Обзорная конференция*, целью которой является рассмотрение функционирования ДНЯО, а также согласование перечня рекомендаций по укреплению Договора. Конференции 2000 и 2010 годов закончились принятием планов действий по ядерному разоружению, однако выполнение многих мер, по которым были заключены договоренности, были провалены.

*Обзорная Конференция 2015 года закончилась безрезультатно* – принятие итогового документа было заблокировано делегациями США, Великобритании и Канады, что еще больше расшатывает основы ДНЯО.

Несмотря на ряд подкрепляющих **ДНЯО** и режим нераспространения механизмов, он **не смог предотвратить появление непризнанных ядерных государств**. Собственные ядерные программы продолжают развивать не подписавшие ДНЯО Израиль, Индия и Пакистан, а также КНДР, которая вышла из ДНЯО в 2003 году и затем с 2006 по 2017 год осуществила шесть ядерных испытаний.

В последнее время наблюдается серьезное **ослабление системы нераспространения ЯО.** *Силовая политика отдельных ядерных держав* (например, силовое вмешательство США в конфликты 1990–2010 годов в Югославии, Ираке и Ливии) *укрепляет в «пороговых» неядерных государствах поддержку идей создания собственного ЯО*, а также средств его доставки. Ряд стран начинают *рассматривать ЯО как весомую гарантию от агрессивных действий и интервенций со стороны других держав в условиях нарастающей дисфункции институтов международной безопасности.*

*С ощущением «дефицита» собственной безопасности связаны в том числе и кризисы вокруг ракетно-ядерных программ КНДР и Ирана. При этом региональные системы безопасности не выстроены должным образом и не могут гарантировать предотвращение безнаказанного вмешательства во внутренние дела.*

**Риск региональной ядерной войны сохраняется.** *Президент США Д. Трамп в мае т. г. объявил о выходе из Совместного всеобъемлющего плана действий в отношении иранской ядерной программы[6], фактически являвшегося важным элементом системы нераспространения. Этот дестабилизирующий шаг способен подтолкнуть Иран к созданию ядерного оружия и активизации ракетных программ.*

Ситуацию отягощает и обозначившийся **кризис режимов контроля над вооружениями.** Заблокировав ратификацию Договора о всеобъемлющем запрещении ядерных испытаний (ДВЗЯИ) и сорвав исполнение соглашения с Россией об утилизации излишков оружейного плутония, **США ослабляют систему нераспространения и ядерного разоружения**.

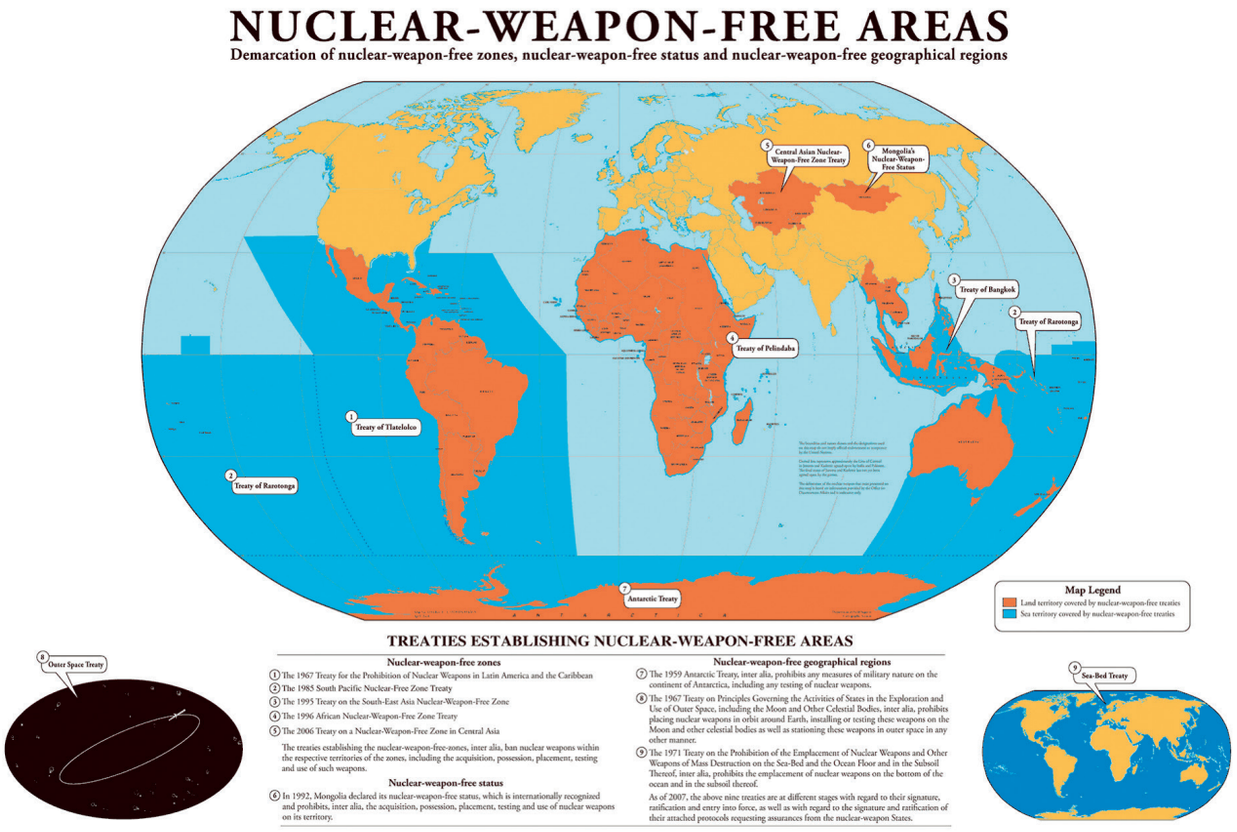
*Недовольство стран, не являющихся членами «ядерного клуба», выразилось в разработке и поддержке 122 странами в июле 2017 года* на ГА ООН *Договора о запрещении ядерного оружия.* Документ запрещает разработку, испытание, хранение, приобретение, транспортировку и использование ЯО. *Если Договор вступит в силу, то он не будет выполняться ядерными державами.* Поэтому он может стать еще одним «яблоком раздора» в системе нераспространения ЯО.

Эволюция режимов нераспространения привела к **формированию зон, свободных от ядерного и иного оружия массового уничтожения** (ЗСОМУ). Такие зоны начали создаваться еще в 1950–60-х годах на основе регио-

[6] President Donald J. Trump is Ending United States Participation in an Unacceptable Iran Deal (https://www.whitehouse.gov/briefings-statements/president-donald-j-trump-ending-united-states-participation-unacceptable-iran-deal/).

*Рисунок 4*

**Безъядерные зоны в современном мире**




***Источник:*** *Управление ООН по вопросам разоружения (UNODA).*

***Примечание:*** *На карте также отмечены: Антарктика (безъядерная зона с 1959 г.), дно морей и океанов (Договор 1971 г.), указано на безъядерный характер космического пространства (Договор о космосе 1967 г.).*

нальных соглашений между странами, по которым участники отказываются от обладания ЯО. На данный момент введены в действие пять договоров о ЗСОМУ (рис. 4): Договор Тлателолко (Южная и Центральная Америка, Карибский бассейн), 1967 год; Договор Раротонга (южная часть Тихого океана), 1985 год; Бангкокский договор (Юго-Восточная Азия), 1995 год; Договор Пелиндаба (Африка), 1996 год; Семипалатинский договор (Центральная Азия), 2006 год.

*Актуальной темой последних лет было создание ЗСОМУ на Ближнем Востоке*, что связано с распространением ядерных технологий в регионе в связи с планами стран региона по созданию ядерной энергетики (Иран, ОАЭ, Египет, Турция, Саудовская Аравия, Иордания). Создание зоны было одним из условий поддержки арабскими странами решения о бессрочном продлении ДНЯО в 1995 году. В 2015 году США, не желая ухудшать отношения с Израилем, заблокировали созыв международной конференции по созданию такой ЗСОМУ.

**Северо-Восточная Азия – регион, в котором создание ЗСОМУ также весьма актуально.** Две страны региона – Япония и Южная Корея – имеют развитую ядерную энергетику и соответствующую инфраструктуру. Северная Корея является «де-факто» ядерным государством. Создание ЗСОМУ в регионе потребует денуклеаризации Северной Кореи с принятием странами региона гарантий безопасности.

Одним из *ключевых документов в развитие идей ДНЯО должен был стать Договор о всеобъемлющем запрещении ядерных испытаний (ДВЗЯИ)*, открытый для подписания с 1996 года. Договором предусматривается расширение зоны запрета на проведение ядерных испытаний, установленной в 1963 году, – атмосфера, космос и подводное пространство – до безусловной, полностью исключающей испытания ЯО. К настоящему времени договор ратифицировали 166 стран. Из-за того, что несколько государств не ратифицировали его (в частности, США и Китай), он до сих пор не вступил в силу.

Серьезную озабоченность, помимо отказа от ратификации ДВЗЯИ, вызывают официально декларированные в обновленном в начале 2018 года «Обзоре ядерной политики» **планы разработки Соединенными Штатами ядерных боезарядов малой мощности**. Такая политика ставит под сомнение приверженность США соблюдению как своих обязательств по статье VI ДНЯО, так и моратория на ядерные испытания.

Уже более 20 лет обсуждается *проект Договора о запрещении производства расщепляющихся материалов (ДЗПРМ)*. Договор мог бы стать мощным практическим инструментом политики нераспространения ЯО. Однако *стороны не могут согласовать начальные условия договора*, в частности вопрос о декларировании и проверках стартовых запасов ядерных материалов. Особую сложность будет представлять декларирование материалов, содержащихся в ядерных боеприпасах.

В январе 2006 года президент России В. Путин предложил использовать для контролируемого *развития мирной атомной энергетики создание международных центров по оказанию услуг ядерно-топливного цикла*. Такие площадки, находящиеся под контролем МАГАТЭ, могли бы содействовать задачам нераспространения и при этом гарантировать поставки ядерных материалов. С 2007 года *Россия и Казахстан реализуют пилотный проект Международного центра по обогащению урана* в г. Ангарске (Россия). С 2010 года под эгидой МАГАТЭ там был создан первый гарантийный запас ядерных материалов.

*Процессы разоружения и нераспространения диалектически взаимосвязаны.* Прогресс в контроле над вооружениями создает стимулы для продвижения в области нераспространения. В настоящее время, однако, *процесс сокращения и ограничения вооружений зашел в тупик.*

## 3.2. Соглашения по контролю над вооружениями

Обеспечение контроля над вооружениями является одним из ключевых условий поддержания международной безопасности.

**Краеугольным соглашением в сфере наступательных ядерных вооружений является заключенный в 2010 году Пражский Договор СНВ между Россией и США,** который установил **потолки для стратегических сил каждой из двух держав** *по числу развернутых носителей и по числу боезарядов на них* в **700** и **1550** единиц соответственно. Участие в этом соглашении обеспечивает сегодня сохранение стратегического паритета и стратегической стабильности между двумя странами.

*Развязанная на Западе антироссийская кампания и неснижающаяся напряженность в российско-американских отношениях (включая санкционный режим против РФ) серьезно затрудняют диалог о сохранении Договора и о дальнейших возможных сокращениях.*

**В 2002 году США в одностороннем порядке вышли из Договора по ПРО 1972 года, который являлся важнейшим элементом системы стратегической стабильности.** Получив тем самым свободу действий, Вашингтон, помимо развития ПРО на национальной территории, развертывает региональные сегменты ПРО в Евро-Атлантическом и Азиатско-Тихоокеанском регионах. Такие намерения, и в особенности *планы создания позиционного района ПРО в Европе, вызвали серьезную озабоченность в России* в связи с тем, что *эти средства могут быть как направлены против стратегических ядерных сил РФ, так и использоваться для нанесения ударов по российской территории.*

**Принципиальной позицией РФ является сохранение стратегического паритета** *с учетом потенциала ПРО США, американского потенциала обычного высокоточного оружия большой дальности, а также перспектив присоединения к пока еще двустороннему диалогу по СНВ третьих стран.*

**Договор о ракетах средней и меньшей дальности** (1987 год) – бессрочное соглашение, предусматривающее ликвидацию и запрещение производства, испытания и развертывания СССР/Россией и США баллистических и крылатых ракет наземного базирования с дальностью от 500 до 5500 км.

Договор **стал важным элементом стратегической стабильности**, так как *ликвидировал определенные односторонние преимущества США, связанные с размещением на территории Европы ракет средней дальности в ядерном оснащении с минимальным подлетным временем до территории России. С возможным стремлением США вернуть эти односторонние преимущества может быть связана возросшая в последнее время критика Договора со стороны Вашингтона и обсуждение возможностей выхода из него. Дальнейшая судьба Договора находится под угрозой.*

**Российская сторона обеспокоена сохраняющимся присутствием в Европе американского ядерного оружия**. В Европе по прежнему размещен американский ядерный арсенал, насчитывающий

**до 200 авиабомб**. Хотя **Россия после распада СССР вывела свои ядерные вооружения на национальную территорию, США не последовали этому примеру**[7].

В качестве одного из препятствий для переговоров по дальнейшим сокращениям тактического ядерного оружия Россия и США рассматривают **отсутствие перспектив по присоединению к этому процессу других ядерных государств**.

С середины 2020-х годов **США планируют начать цикл полного обновления своих стратегических ядерных сил** (стратегической ядерной триады)[8]. **Расходы на программу, рассчитанную на 30 лет, составят около 1,2 трлн долл. Модернизацию своих ядерных сил проводит и Россия**.

В случае проблем с заключением нового договора или не продлением срока действия Пражского договора намечаемые программы могут быть пересмотрены в сторону увеличения числа стратегических систем и боезарядов, что может создать **потенциальные условия для новой гонки вооружений**.

В настоящее время ведущие военные державы мира развертывают **значительное количество** разнообразных **ударных систем большой дальности**, прежде всего **высокоточных конвенциональных вооружений, способных поражать цели, которые в прошлом можно было уничтожить только с использованием ядерных боеприпасов. В США** эти планы реализуются в рамках **концепции неядерного быстрого глобального удара**.

Аналогичные вооружения создаются в России и КНР.

Введение ограничений в этой области стоит на повестке дня.

**Ведущие военные державы активно осуществляют разработки и частичное развертывание систем вооружения нового поколения,** к которым относятся высокоточные крылатые ракеты, беспилотные системы воздушного, наземного и подводного базирования, а также кибероружие, которые **будут оказывать влияние на** военный баланс и **стратегическую стабильность**. Однако на международном уровне **пока не выработано подходов к ограничению подобных систем**.

Сохраняется реальная **угроза вооружения космического пространства**, поскольку международное право, в соответствии с Договором о космосе 1967 года, напрямую не запрещает размещения в космосе любого оружия, кроме оружия массового уничтожения.

**Россия последовательно борется против милитаризации космического пространства.** В 2004 году Россией **в одностороннем порядке объявлено об отказе размещать оружие в космосе первой.**

В 2008 году Россия и Китай на Конференции по разоружению в Женеве официально внесли проект Договора о предотвращении размещения оружия в космическом пространстве, применения силы или угрозы силой в отношении космических объектов (ДПРОК). Однако **США блокируют переговоры**, поскольку **Вашингтон** традиционно **не устраивают перспективы любых ограничений военно-космической деятельности**.

Начиная с 1999 года страны Запада под разными предлогами затягивали процесс ратификации *Соглашения об адаптации* (1999 год), *Договора об обычных вооруженных силах в Европе* 1990 года. Тем временем НАТО прошло через несколько волн расширений, что увеличивало «перекос» в численности обычных вооружений в пользу альянса. В этой ситуации в 2015 году Россия была вынуждена полностью приостановить свое участие в Договоре.

**Процесс расширения НАТО на Восток и приближения военной инфраструктуры альянса к российским границам на протяжении многих лет является фактором, осложняющим диалог России со странами Запада в сфере «жесткой безопасности»**.

**Украинский кризис 2014 года был использован Западом для укрепления и наращивания силовой составляющей по линии НАТО и размещения военных контингентов альянса вблизи западных рубежей России, что серьезно обострило военно-политическую ситуацию в Европе**.

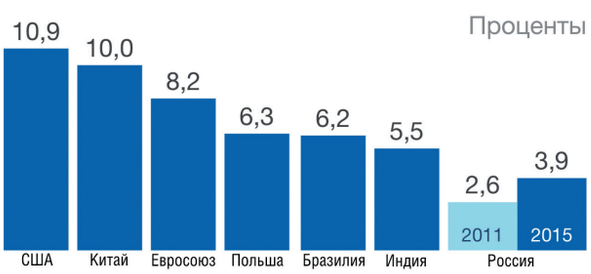
## 4. ИКТ-технологии и развитие цифровой экономики

«Цифровая экономика» формирует новую структуру информационного пространства и новые модели производственных отношений, основанные на цифровых платформах, охватывает глобальные рынки и весь отраслевой состав мировой экономики. Технологии и платформы цифровой экономики формируют среду для ее активного самовоспроизводства и масштабирования.

Доля цифровой экономики в ВВП США и Китая достигает 10 %, Евросоюза – 8 %, России – около 4 % (рис. 5). При этом, по прогнозам экспертов, уже в ближайшие годы доля цифровой экономики может стремительно возрасти.

*Рисунок 5*

**Доля цифровой экономики в ВВП в 2015 г.**




***Источник:*** *доклад 2017 г. Цифровая Россия: новая реальность. (https://www.mckinsey.com/~/media/McKinsey/Locations/Europe%20and%20Middle%20East/Russia/Our%20Insights/Digital%20Russia/Digital-Russia-report.ashx).*

В экономико-технологической сфере развитых государств мира уже запущен цикл четвертой промышленной революции (Индустрия 4.0), связанный с конвергенцией и внедрением нано-, био-, инфо- и когнитивных технологий (NBIC).

Наиболее обширной и динамичной в этом «квартете» является группа информационно-телекоммуникационных технологий (ИКТ), к которым относятся такие новые технологические явления, как обработка больших

[7] МИД призвал США вывести ядерное оружие из Европы, 18 декабря 2017 г. (https://topwar.ru/132210-midprizval-sshavyvesti-yadernye-vooruzheniya-izevropy.html).

[8] Стратегическая ядерная триада включает в себя три компонента: стратегическую авиацию, межконтинентальные баллистические ракеты и атомные подводные лодки, оснащенные баллистическими и крылатыми ракетами подводного базирования.

*Рисунок 6*

**Годовой вклад Интернета вещей в мировую экономику к 2025 г.**

***Источник:*** *доклад 2017 г. Цифровая Россия: новая реальность. (https://www.mckinsey.com/~/media/McKinsey/Locations/Europe%20and%20Middle%20East/Russia/Our%20Insights/Digital%20Russia/Digital-Russia-report.ashx)&*

данных (bigdata), Интернет вещей, распределенный реестр, искусственный интеллект, квантовые вычисления, дополненная и виртуальная реальность, и др.

В 2017 году производство товаров и услуг ИКТ составило примерно 6,5 % валового мирового продукта (ВВП), и около 100 млн человек были заняты в секторе услуг ИКТ[9]. По некоторым оценкам[10], к 2020 году общее число устройств Интернета вещей составит 50 млрд единиц. Годовой вклад Интернета вещей в мировую экономику может составить от 4 до 11 трлн долл. США к 2025 году (рис. 6).

Переход глобальной экономики к новому технологическому укладу на фоне магистрального тренда на массовое освоение ИКТ-среды и цифровизацию всех сфер человеческой деятельности является ключевым процессом, определяющим особенность современного этапа мирового развития.

Объективное явление смены вех на стыке уходящего и нарождающегося технологических укладов открывает широкий горизонт новых возможностей для прорывного экономического развития и одновременно таит существенные риски.

От того, насколько эффективно национальные экономики воспользуются открытыми в период перехода к новому технологическому укладу окнами возможностей опережающего развития, будет зависеть распределение бонусов по итогам данных переходных процессов, которое, в конечном счете, может сказаться на конфигурации центров экономического могущества в мире.

Все будет зависеть от степени эффективности усилий как на национальном (структурное реформирование экономик для адаптации к новому технологическому укладу, инвестиционные программы развития инновационных секторов и внедрения новых технологий, формирование стимулирующего правового регулирования), так и на международном уровне (обеспечение равного доступа к использованию возможностей нового технологического уклада).

В России, в соответствии со Стратегией научно-технологического развития, в ближайшие 10–15 лет предполагается переход к передовым цифровым, интеллектуальным технологиям, системам обработки больших объемов данных и другим новым технологиям. План такого перехода содержится в программе «Цифровая экономика Российской Федерации».

В ней выделено пять базовых направлений усилий по развитию цифровой экономики на период до 2024 года: нормативно-правовое регулирование, кадры и образование, формирование исследовательских компетенций и технических заделов, информационная инфраструктура и информационная безопасность.

Принятие аналогичных программ поддержки цифровой экономики практикуется рядом государств. В частности, в США с 2016 года реализуется «Повестка дня цифровой экономики»[11].

В большинстве национальных программ развития цифровой экономики приоритетное внимание уделяется задаче обеспечения информационной безопасности. Ввиду трансграничности и комплексного характера информационных угроз условием поступательного развития национальных компонентов глобальной цифровой экономики является налаживание эффективного международного сотрудничества в сфере обеспечения информационной безопасности.

---

[9] Доклад об информационной экономике за 2017 год // ЮНКТАД [Официальный сайт] (http://unctad.org/en/PublicationsLibrary/ier2017_overview_ru.pdf).

[10] Интернет вещей: Как изменится вся наша жизнь на очередном витке развития Всемирной сети // CISCO [Officialwebsite] (https://www.cisco.com/c/dam/global/ru_ru/assets/executives/pdf/internet_of_things_iot_ibsg_0411final.pdf).

[11] Commerce Department Digital Economy Agenda 2016 // National Telecommunications and Information Administration United States Department of Commerce [Official website] (https://www.ntia.doc.gov/files/ntia/publications/alan_davidson_digital_economy_agenda_deba_presensation_051616.pdf).

# 5. Обеспечение международной информационной безопасности

*Информационно-коммуникационные технологии становятся сегодня не только основным драйвером цифрового развития, но также превращаются в определяющий военно-политический фактор – неотъемлемый элемент современного военного потенциала государств (киберпотенциал),* дополняющий, а иногда и заменяющий обычные военные средства. ИКТ также широко применяются террористическими и криминальными структурами.

В силу взаимосвязанности глобальных информационных сетей ни одна страна в мире не может считать себя защищенной от трансграничных информационных угроз и не в состоянии в одиночку гарантированно обеспечивать информационную безопасность. Этим обуславливается активное развитие международного сотрудничества в сфере информационной безопасности и кибербезопасности.

*Кибербезопасность трактуется как обеспечение целостности, конфиденциальности и доступности данных в глобальной ИКТ-среде.*

Российская Федерация продвигает создание инклюзивной системы *международной информационной безопасности (МИБ) в более широкой трактовке.* Система МИБ призвана *обеспечивать такое состояние глобального информационного пространства, при котором надежно защищены права личности, общества и государства в информационной сфере, а также элементы критической информационной инфраструктуры.*

## 5.1. Основные угрозы в информационном и киберпространстве

*Наиболее острые угрозы информационной безопасности для современных государств* связаны с развитием:

- ***информационного и кибероружия, в том числе кибершпионажа;***
- ***киберпреступности;***
- ***кибертерроризма.***

В фокусе особого внимания – *проблематика кибератак на элементы критически важной инфраструктуры (КИ), а также развитие на базе ИКТ инструментов «мягкой силы» для вмешательства во внутренние дела государств.*

Противодействие угрозам в ИКТ-среде осложняется ее трансграничностью, анонимностью. безуликовостью (отсутствие материальных следов в качестве юридического доказательства), стремительностью развития процессов, а также сложностями выработки международно-правовых механизмов предупреждения, выявления, расследования и привлечения виновных к ответственности.

На текущий момент в мире достаточно широко ведутся разработки *кибероружия*. Еще в конце 1990-х годов Конгрессом США была озвучена информация, что 120 стран разрабатывают информационное оружие[12]. За последние 5–10 лет многие ведущие государства мира создали кибервойска (или войска информационной безопасности). Помимо США, в десятку передовых стран в этой области входят Великобритания, Франция, Германия, Россия, Китай, Израиль, Южная Корея, КНДР.

Принятая в 2015 году США Стратегия кибербезопасности нацелена не только на *кибероборону*, но и на ведение наступательных кибероперациий[13]. В Стратегии национальной безопасности США 2017 года указывается, что «Соединенные Штаты будут сдерживать, защищать и, когда это необходимо, побеждать злонамеренных субъектов, которые используют киберпространство против Соединенных Штатов»[14].

*Страны ЕС/НАТО активно наращивают свой киберпотенциал. В структуре НАТО с 2008 года действует центр кибероборонь.*

Серьезной угрозой в контексте стремительного развития информационного и кибероружия является риск провоцирования полномасштабных межгосударственных конфликтов, в первую очередь из-за отсутствия механизмов быстрой и точной атрибуции атак, а также возможности несоразмерного реагирования на угрозы (пострадавшая сторона в случае тяжких последствий кибератаки, например вывода из строя критической инфраструктуры, может применить в ответ физическое оружие, причем государственная принадлежность источника угрозы, как правило, является недоказуемой). В настоящее время не выработаны международные нормативно-правовые критерии отнесения кибератак к вооруженному нападению. Данные риски существенно возросли в связи с объявлением американским представителем на Варшавском саммите НАТО в июле 2016 года о возможности применения ст. 5 Вашингтонского договора в ответ на кибернападения на стран - членов альянса.

Критические масштабы приобретает и угроза киберпреступности, наносящей неприемлемый ущерб экономическим интересам государства, граждан и бизнеса. Отмечается тенденция неуклонного возрастания *совокупного мирового урона от киберпреступности – если в 2015 году он составлял 3 трлн долл., то к 2021 году прогнозируется его рост минимум до 6 трлн долл. в год*[15].

Этапным достижением в этой сфере можно считать принятие в 2001 году Конвенции Совета Европы по киберпреступности[16], содержащей предложение имплементировать в законодательство стран-участниц единые нормы об уголовной ответственности за киберпреступления. Однако практическая действенность этого документа ограничена, т. к. часть стран усматривает в ряде положений конвенции нарушение принципа национального суверенитета (в частности, пункт о проведении оперативно-следственных мероприятий в информационной инфраструктуре государств без их

[12] Крутских А. В. Война или мир: международные аспекты информационной безопасности / Научные и методологические проблемы информационной безопасности, под ред. В. П. Шерстюка. – М., 2004.

[13] DOD Cyber Strategy 2015 (https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf).

[14] National Security Strategy of the United States of America. December 2017. (https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf).

[15] Cybercrime Damages $6 Trillion by 2021 (https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/).

[16] Convention on cybercrime, Council of Europe (http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm).

согласия, ст. 32-б). При этом конвенция устаревает ввиду появления новых технологий и разновидностей киберпреступлений.

В 2017 году Россией на ГА ООН был представлен проект конвенции «О сотрудничестве в сфере противодействия информационной преступности». Проект в основном учитывает недостатки конвенции Совета Европы, предусматривает широкий современный понятийный аппарат и криминализацию появляющихся новейших форм киберпреступности.

Фактором, серьезно затрудняющим разработку международных документов по кибертерроризму, является отсутствие международно признанного определения терроризма и единых перечней ТО.

Группа правительственных экспертов ООН (ГПЭ ООН) в целях противодействия использованию ИКТ в террористических целях рекомендует «расширить обмен информацией и оказание взаимопомощи в целях преследования террористов и пресечения случаев преступного использования ИКТ»[17].

Значимой частью проблемы является развитие теневого рынка вредоносного программного обеспечения. Преступные синдикаты активно привлекают экспертов к разработке соответствующих средств для использования уязвимостей в ПО[18].

Обеспокоенность большинства государств опасностью кибератак на критически важную инфраструктуру (в том числе органы государственной власти, электроэнергетическая, нефтегазовая, транспортная, финансовая системы, водоснабжение, ядерные объекты, военно-промышленный комплекс) обусловлена тем, что выведение из строя незащищенных объектов такого рода способно привести к цепной реакции и быстрому наступлению катастрофических последствий, представляющих полномасштабную угрозу национальной безопасности. При этом автоматизированные системы управления объектов КИ остаются потенциально уязвимыми для кибератак, даже если они напрямую не подключены к сети Интернет.

Значительные опасения вызывает также *тенденция развития на новой технологической базе ИКТ эффективных инструментов «мягкой силы», направленных на вмешательство во внутренние дела государств*. В этих целях могут использоваться кибервоздействие на промышленные и финансовые объекты, кибершпионаж с целью дискредитации неугодных политических сил, а также сетевые технологии направленного информационного воздействия (группы в социальных сетях/мессенджерах) с целью манипуляции общественным мнением, а также подготовки и осуществления массовых протестных акций. На протяжении последних десятилетий растет интенсивность применения такого рода технологий как в ходе вооруженных конфликтов (в Афганистане, Ираке, Ливии и Сирии), так и в ходе так называемых цветных революций (Грузия, 2003 год; Украина, 2004 и 2014 годы; Киргизия, 2005 год; Египет, 2011 год, и др.).

## 5.2. Международное сотрудничество в области МИБ и кибербезопасности

Ведущими странами мира в настоящее время продвигается два базовых подхода к обеспечению безопасности в ИКТ-среде. США и западные страны, включая страны ЕС/НАТО, развивают стратегии кибербезопасности, в которых акцент делается на обеспечение безопасности информации в киберпространстве.

В свою очередь Россией, Китаем и другими странами БРИКС, ШОС и ОДКБ предлагается более комплексная и инклюзивная концепция международной информационной безопасности, в рамках которой учитывается также угроза направленного информационного воздействия с использованием ИКТ для влияния на социально-политические процессы и вмешательства во внутренние дела суверенных государств.

На протяжении последних лет концепция МИБ находит широкую поддержку. В ОДКБ развивается процесс гармонизации национального законодательства государств-членов в сфере обеспечения информационной безопасности и противодействия правонарушениям в информационной сфере. В ШОС с 2009 года действует соглашение о сотрудничестве в информационном пространстве[19]. Вопрос заключения подобного соглашения прорабатывается и в рамках БРИКС[20].

Еще в 1998 году, на 53-й сессии Генеральной Ассамблеи (ГА) ООН по инициативе Российской Федерации консенсусом была принята резолюция «Достижения в сфере информатизации и коммуникаций в контексте международной безопасности» (A/RES/53/70). Эта резолюция выделяла три основные сферы ИКТ-угроз (связанные с применением в военных, террористических и преступных целях) и призывала к определению основных понятий и разработке международных принципов поведения государств в ИКТ-сфере.

ООН является эффективной площадкой для проработки проблем безопасности ИКТ-среды. По решению 56-й сессии ГА ООН (2001 год) была создана ГПЭ по вопросам информатизации и телекоммуникаций в контексте международной безопасности. В 2015 году в докладе ГПЭ сформулированы правила, принципы и нормы ответственного поведения государств в ИКТ-среде. Однако согласование порядка применения этих норм и правил в 2016 году столкнулось с невозможностью достичь консенсуса.

Основное концептуальное отличие российского и американского подходов по данному вопросу состоит в том, что *с точки зрения России конфликты в ИКТ-среде недопустимы, следовательно, они подлежат не регулированию, а профилактике, предотвращению или пресечению*. Страны Запада при этом исходят из необ-

[17] Доклад ГПЭ по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности 2015 г. (http://www.un.org/ru/documents/ods.asp?m=A/70/174).

[18] DOD Cyber Strategy 2015. P. 2.

[19] Соглашение между правительствами государств – членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности от 16 июня 2009 года (http://base.spinform.ru/show_doc.fwx?rgn=28340).

[20] БРИКС может выработать соглашение об информационной безопасности (http://tass.ru/mezhdunarodnaya-panorama/4443112).

ходимости регулирования военно-политического использования ИКТ, что, как следствие, может повлечь легитимизацию применения кибероружия и военной силы в ответ на кибератаки.

Базовые элементы позиции США по международному сотрудничеству в сфере кибербезопасности определены в выдвинутой США в 2011 году Международной стратегии для киберпространства[21]. Ее целью декларируется создание единой платформы взаимодействия для государств, придерживающихся сходной с США позиции по вопросам безопасности и использования киберпространства. Данный документ фактически носит неуниверсальный характер и ориентирован, прежде всего, на сотрудничество со странами ЕС и НАТО, а также со странами – участниками Соглашения о радиотехнической разведывательной деятельности (Великобритания, Канада, Австралия, Новая Зеландия).

В 2011–2013 годах США поддержали отдельные инициативы России в сфере информационной безопасности. В 2013 году подписано Совместное заявление президентов Российской Федерации и Соединенных Штатов Америки о новой области сотрудничества в укреплении доверия.

Однако впоследствии *США перешли к блоковому конфронтационному курсу в сфере информационной безопасности и уклоняются от взаимодействия с Россией в сфере предотвращения инцидентов в ИКТ-среде, предусмотренного в совместном заявлении президентов России и США*[22]. США также отказались от договоренности, достигнутой в ходе встречи президентов двух стран на полях G-20 в июле 2017 года, о создании рабочей группы по кибербезопасности. В опубликованном в июле 2016 года исследовании Комитета начальников штабов ВС США «Общая оперативная обстановка 2035» Россия и Китай, наряду с Ираном и КНДР, отнесены к главным противникам США в киберпространстве.

## 6. Опыт межпарламентских ассамблей СНГ и ОДКБ в противодействии терроризму, экстремизму и другим современным угрозам и вызовам

В рамках Содружества независимых государств (СНГ) и Организации Договора о коллективной безопасности (ОДКБ) – международных организаций, образованных государствами постсоветского пространства, – активно действуют структуры межпарламентского взаимодействия.

Раз в полгода в Санкт-Петербурге созываются сессии Межпарламентской Ассамблеи (МПА) СНГ, на которых около 500 делегатов парламентов стран-участниц работают над модельными законами, призванными гармонизировать национальные законодательства в рамках интеграционного объединения. В работе МПА участвуют парламентарии девяти стран СНГ[23], а также Афганистана как государства-наблюдателя.

После создания в 2002 году ОДКБ была сформирована Парламентская Ассамблея ОДКБ (ПА ОДКБ). На сегодняшний день приняты 38 модельных законов ОДКБ.

ПА ОДКБ принято Обращение к парламентам государств мира и международным парламентским организациям об объединении усилий в противодействии терроризму и иным формам насильственного экстремизма на современном этапе, в котором приветствуется установление контактов с парламентами государств-членов и наблюдателей Шанхайской организации сотрудничества (ШОС).

Приняты Рекомендации по сближению национального законодательства государств ОДКБ по противодействию терроризму и экстремизму.

Осуществляется гармонизация правового регулирования государств – членов ОДКБ в ИКТ-сфере.

*Приняты и внедряются Рекомендации по всему спектру законодательной работы в области информационной безопасности.*

В большинстве стран – членов ОДКБ приняты комплексы взаимосвязанных законов, регулирующих развитие информационной сферы: законы о защите электронных данных, о цифровой подписи, о защите авторских прав в цифровой сфере, о противодействии экстремизму и терроризму в информационном пространстве.

На развитие законодательства стран ОДКБ о противодействии терроризму и экстремизму оказали влияние результаты модельного законотворчества в рамках СНГ.

Основу модельной законодательной базы по контртерроризму составлял закон «О борьбе с терроризмом» (в редакции 2004 года). Затем были приняты модельные законы «О противодействии организациям и лицам, деятельность которых имеет целью осуществление актов терроризма на территориях других государств» (2004 год), «О противодействии финансированию терроризма» (2006 год), «О противодействии легализации («отмыванию») доходов, полученных преступным путем, и финансированию терроризма» (2008 год).

Утверждены Рекомендации по правовому регулированию эксплуатации открытых телекоммуникационных сетей для предупреждения их использования в террористических и иных противоправных целях.

С этими задачами тесно смыкается и группа модельных законов, посвященных промышленной и транспортной безопасности: «О контроле за оборотом радиоактивных материалов» (2004 год), «О безопасности на транспорте» и «О безопасности на воздушном транспорте» (2007 год).

---

[21] International Strategy for Cyberspace (https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/internationalstrategy_cyberspace.pdf).

[22] Совместное заявление президентов Российской Федерации и Соединенных Штатов Америки о расширении двустороннего взаимодействия. URL: http://kremlin.ru/events/president/news/18355.

[23] В деятельности МПА приостановили участие представители Украины, которая начала процедуру выхода из Содружества.

Приняты Рекомендации по унификации и гармонизации национальных законодательств по обеспечению химической и биологической безопасности.

Группа модельных законов по борьбе с экстремизмом представлена законом «О противодействии экстремизму», разработанным в 2009 году.

Также приняты Рекомендации по совершенствованию законодательства государств – участников СНГ в сфере противодействия экстремизму (2013 год).

Линии модельного законодательства по борьбе с незаконным оборотом наркотиков положил начало закон «О наркотических средствах, психотропных веществах и их прекурсорах» (2006 год).

Приняты Рекомендации по унификации и гармонизации национального законодательства государств – участников СНГ в сфере борьбы с незаконным оборотом наркотических средств, психотропных веществ и их прекурсоров (2006 год).

Шанхайская организация сотрудничества, образованная в 2001 году[24], переживает период формирования парламентского измерения своей деятельности. В ШОС с 2006 года функционирует Совещание руководителей парламентов. Данный формат подтвердил свою востребованность и хорошо подходит для обсуждения межпарламентского взаимодействия стран ШОС в сфере безопасности, включая вопросы противодействия терроризму, экстремизму, а также международной информационной безопасности.

В 2009 году ШОС приняла Конвенцию против терроризма и Положение о политико-дипломатических мерах и механизмах реагирования на ситуации, ставящие под угрозу мир, безопасность и стабильность в регионе. За последние несколько лет по итогам саммитов ШОС приняты Душанбинская (2014 год), Уфимская (2015 год), Ташкентская (2016 год) и Астанинская (2017 год) декларации, зафиксировавшие общие подходы государств ШОС к противодействию терроризму, экстремизму и угрозам МИБ.

В ходе дальнейшего развития парламентского измерения ШОС предполагается активизация работы по согласованию и гармонизации законодательства, в том числе *в области региональной безопасности, борьбы с экстремизмом и терроризмом, безопасности ИКТ-среды*.

Примеры усилий по гармонизации национальных законодательств в сфере обеспечения безопасности в рамках СНГ, ОДКБ, а в перспективе – ШОС указывают на объективную необходимость активизации продуктивного межпарламентского сотрудничества в области противодействия глобальным вызовам и угрозам.

Опыт межпарламентских ассамблей СНГ и ОДКБ может быть широко использован парламентскими структурами других региональных интеграционных объединений.

[24] Ее членами являются Индия, Казахстан, КНР, Киргизия, Пакистан, Россия, Таджикистан и Узбекистан.

# ОСНОВНЫЕ ВЫВОДЫ

## Совместная политическая работа

Международное парламентское движение обладает значительным политическим потенциалом влияния на мировые дела, раскрытие которого возможно через более активное позиционирование в качестве проводника:

- снижения конфронтации и конфликтного потенциала в мире;
- деэскалации напряженности в международных отношениях;
- конструктивного, прагматичного и продуктивного сотрудничества между государствами и их объединениями в интересах укрепления международной и региональной безопасности и стабильности;
- утверждения коллективных начал в мировых делах и объединительной повестки противодействия традиционным и новым вызовам и угрозам;
- урегулирования разногласий и устранения возникающих угроз миру на основе диалога при неукоснительном соблюдении основополагающих норм международного права, принципов уважения суверенитета государств, невмешательства в их внутренние дела;
- утверждения принципов ответственного поведения в мировом информационном пространстве и формирования режима безопасности ИКТ-среды, позволяющего предотвращать в ней в том числе межгосударственные инциденты;
- культуры соблюдения договоров и режимов по контролю над вооружениями и ядерному нераспространению как базового фактора военно-политической стабильности;
- отказа от односторонних попыток решения международных споров с применением силы или санкционного давления.

## Совместная законотворческая и контрольная работа

Совершенствование координации и гармонизации на основе обмена опытом и лучшими практиками национальных законодательств, средств и методов парламентского контроля в ключевых областях безопасности:

- противодействии международному терроризму;
- комплексной борьбе с наркотрафиком;
- обеспечении безопасной ИКТ-среды, эффективного купирования всего спектра киберугроз – от киберпреступности до кибератак на объекты критической инфраструктуры;
- обеспечении бесперебойной работы национальных систем сохранности ядерных материалов, защиты ядерных объектов и опасных производств.