

Глобальные ИКТ-угрозы и проблемы безопасности в военно-политической сфере

Global ICT Threats and Security Issues in Military Political Sphere

Prof. Nataliya P. Romashkina

Head of the Informational Security Problems Department of the

IMEMO named Primakov,

Corresponding member of the Military Sciences Academy

+7 926 247 46 25

Romachkinan@yandex.ru

Moscow 2019

ИКТ

ИКТ (информационно-коммуникационные технологии) –

процессы и методы взаимодействия с информацией с применением устройств вычислительной техники и телекоммуникации

ICT

ICT (information and communication technologies)

are processes and methods of interaction with information, using computer devices, as well as telecommunications

Глобальные проблемы МИБ

3

- 1** Наступательные ИКТ-вооружения
- 2** «Мягкая сила» с применением ИКТ во враждебных военно-политических целях
- 3** ИКТ для пропаганды и рекрутинга экстремизма и терроризма
- 4** ИКТ для нападений на критическую инфраструктуру государств
- 5** Снижение уровня стратегической стабильности

Global Problems of International Information Security

- 1** Offensive ICT-weapons
- 2** “Soft power” using ICT for hostile military and political purposes
- 3** ICT for propaganda and recruitment of extremism and terrorism
- 4** ICT for attack on Critical National Infrastructure
- 5** Decrease in level of strategic stability

**Проблема обеспечения ИКТ-
безопасности на критически
важных объектах
инфраструктуры государства
(КИ)**

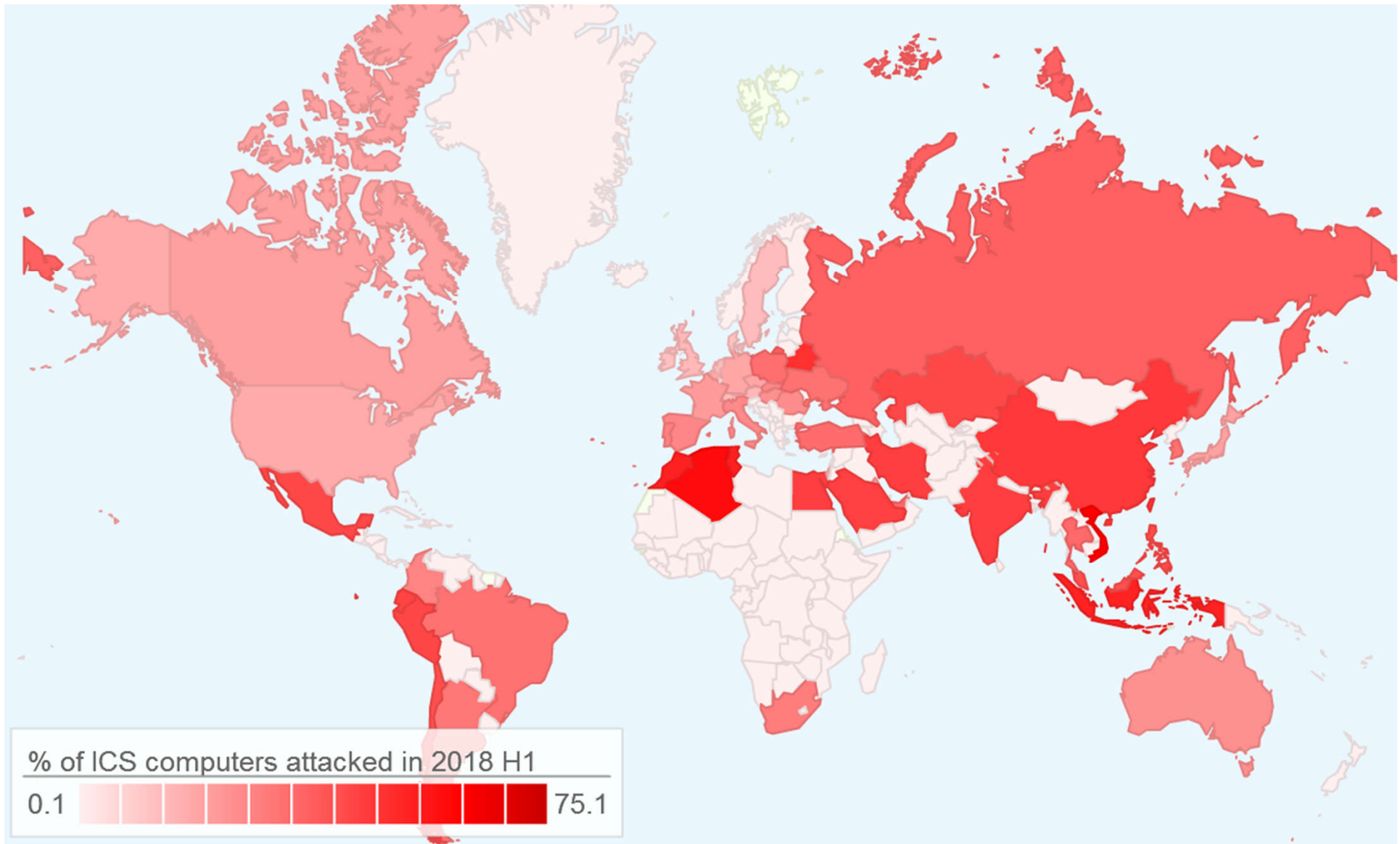
**ICT Security of Critical
National Infrastructure (CI)
Problem**

CNI – systems and tools that are so vital to a state that disruption or destruction has an irreversible negative impact on national and economic security, health, law, etc.

CNI Security – protection against the threats from special information technologies for destruction or for inadmissible use of these objects

География атак на системы промышленной автоматизации

Geography of Attacks on Industrial Automation Systems



**Проблема ИКТ-безопасности
военных объектов
как части КИ**

**Problem of ICT Security of
Military Objects
as Part of CI**

Борьба с системами управления и контроля

Command and control warfare (C2W)

Разведывательное противоборство

Intelligence based warfare (IBW)

Электронное противоборство

Electronic warfare (EW)

*Военные средства, способствующие проведению
информационных операций*

Supporting information operations defense technology

ИКТ-угрозы в военной сфере

Все ИКТ-угрозы можно отнести к различным элементам военной организации и инфраструктуры

Блок ИКТ-угроз в сфере ЯО – важнейший!

ICT Threats in Military Sphere

All ICT threats can be traced back to different military organization and infrastructure elements

The most important – in nuclear weapons sphere!

8

Эскалация конфликта

Conflict Escalation

Вчера

Yesterday



**Эскалация
конфликта с ИКТ**

**Conflict
Escalation with ICT**

9

Новая реальность

New Reality

**Снижение уровня
кризисной стабильности**



**Decrease of
Crisis Stability Level**

Конфликт

of interest



**Эскалация
конфликта с ИКТ
Новая реальность**

**Conflict
Escalation with ICT
New Reality**

**Снижение уровня
стратегической стабильности**



**Decrease of
Strategic Stability Level**

11

**Наличие
у страны-жертвы
информации
о планах кибератаки**

**Victim state is informed
about the planned
cyber attack**

**Снижение уровня
кризисной стабильности**



**Decrease
of Crisis Stability Level**

Конфл

Interest

**Эскалация
конфликта с ИКТ**

**Conflict
Escalation with ICT**

12

Новая реальность

New Reality

**Снижение уровня
стратегической стабильности**



**Decrease of
Strategic Stability Level**

Конфликт

Interest



Равная уязвимость

Equal Vulnerability

13

► Страны с наиболее развитой ИКТ-сферой наиболее уязвимы

► Возможность взаимного применения ИКТ против КИ и в военно-политических целях для враждебных действий и актов агрессии

► Опасность для лидера ИКТ-противоборства: контроль и дезинформация со стороны компетентного противника

► Countries with the most advanced ICT are the most vulnerable

► Possibility of mutual use of ICT against CI and for military and political purposes for hostile actions and acts of aggression

► Danger for the ICT-leader of confrontation: control and misinformation by a competent opponent

Что делать?

14

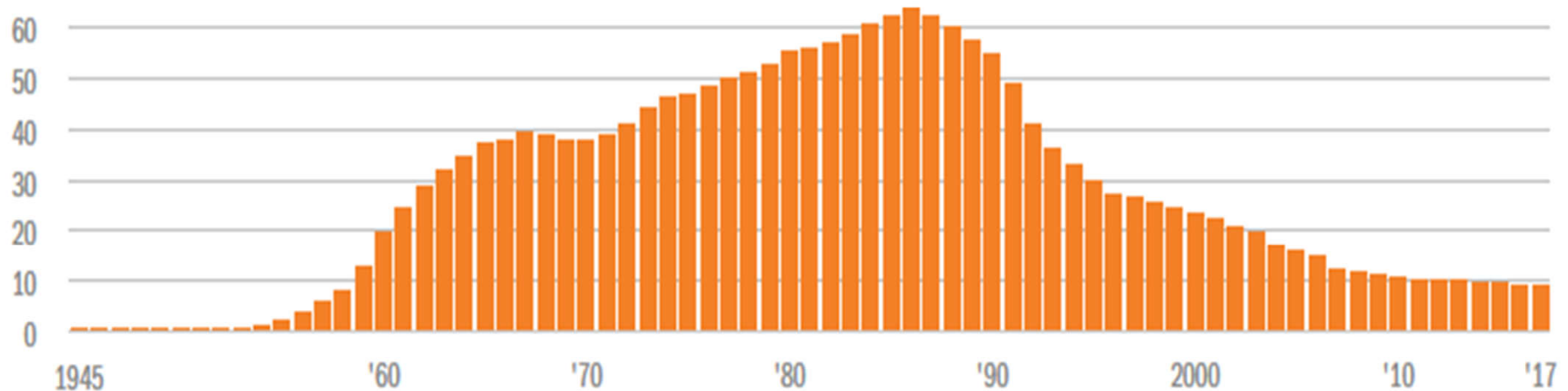
1. Переговоры по ограничению и сокращению стратегических ядерных вооружений

What to Do?

1. Bilateral (Russia-US) and multilateral negotiations on the limitation and reduction of strategic nuclear weapons

GLOBAL NUCLEAR WEAPONS

TOTAL NUCLEAR WARHEADS in thousands



Source: Bulletin of the Atomic Scientists

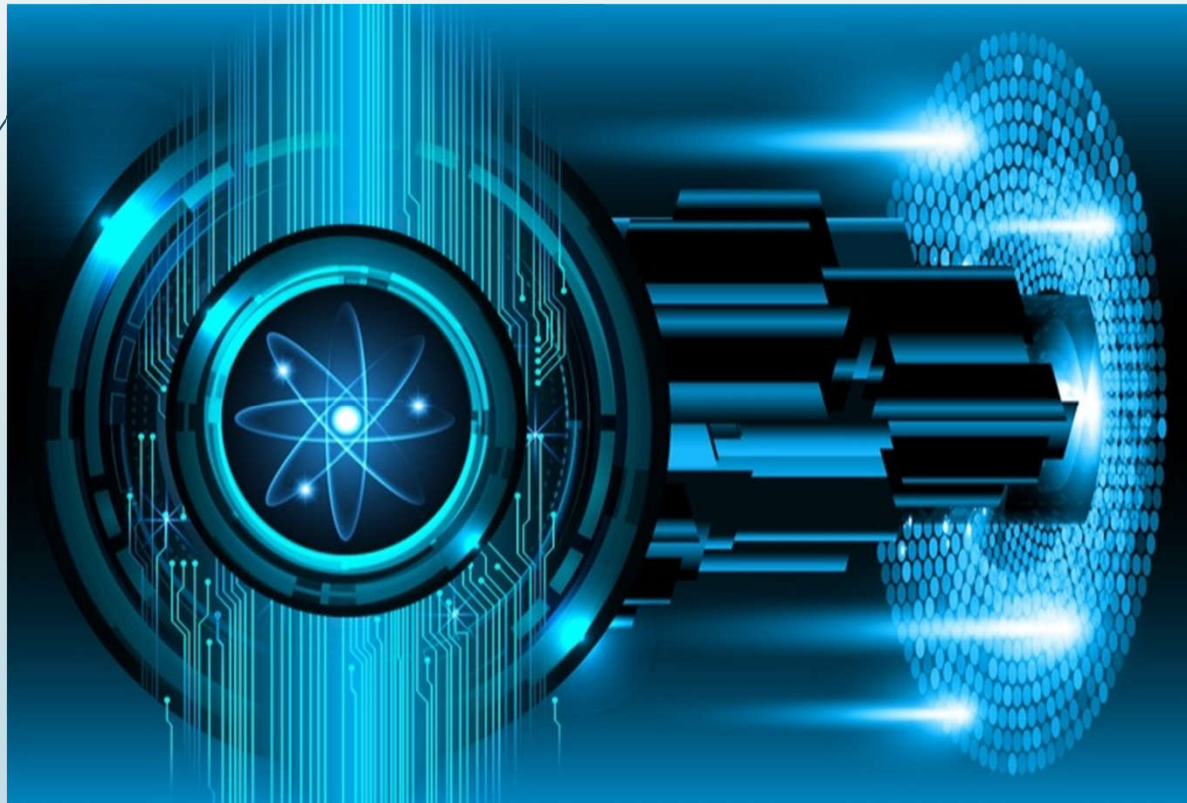
Что делать?

15

2. Включать проблемы ИКТ в переговоры по ЯО и стратегической стабильности

What to Do?

2. To include ICT security in negotiations on nuclear arms and strategic stability with Russia



Что делать?

16

3. Меры по укреплению доверия в сфере ИКТ



What to Do?

3. Trust-building approaches in ICT field



Что делать?

4. Государствам с ЯО:

1 Совершенствовать

- 1) ИКТ-безопасность КИ, военных объектов;
- 2) эффективность подготовки персонала

2

Обеспечивать боевую устойчивость ВС (стратегических сил сдерживания) в условиях деградации объектов техносферы

What to Do?

4. For nuclear states:

1 To improve

- 1) CI and military infrastructure security;
- 2) effectiveness of personnel training

2

To ensure combat stability of armed forces (especially, strategic deterrence forces) in conditions of degradation of techno-sphere objects

Что делать?

18

5. Международные теоретические, методологические и практические исследования стратегической стабильности

What to Do?

5. International theoretical, methodological and practical academic research on strategic stability



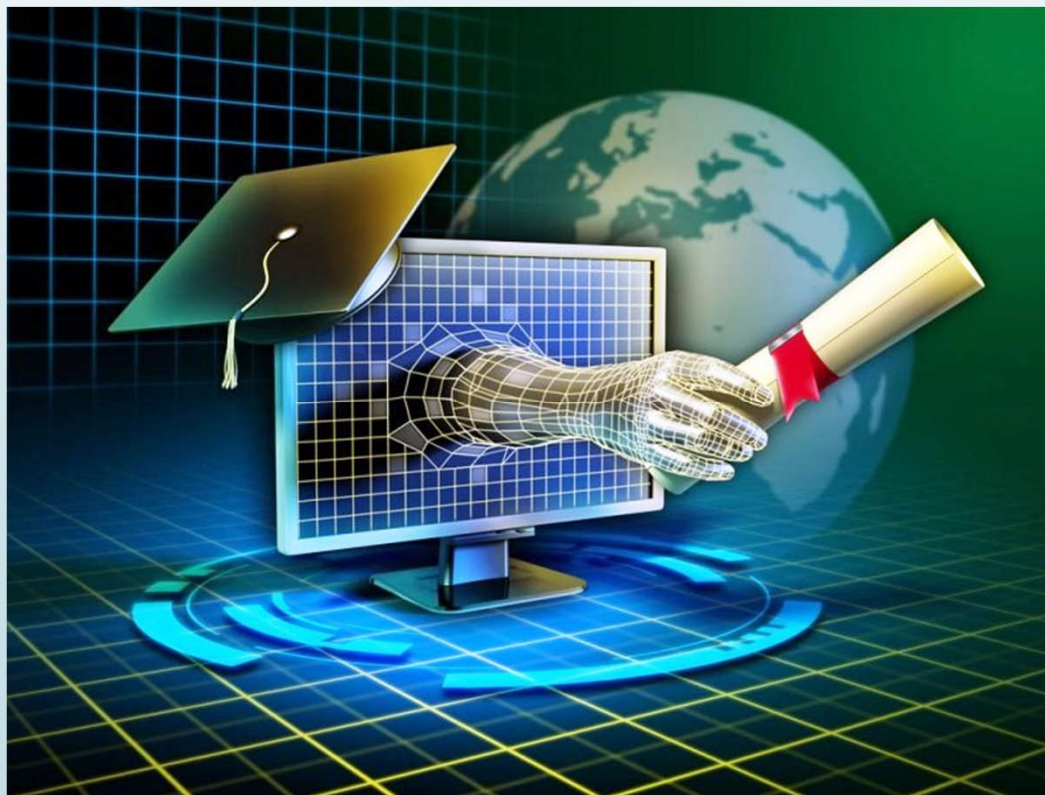
Что делать?

19

6. Международные научно-экспертные проекты для обсуждения проблем организации партнерства в области ИБ

What to Do?

6. International scientific and expert projects on problems of partnership in information security field



Организация Объединенных Наций

Что делать?

**7. Международный
режим под
контролем ООН**



What to Do?

**7. International
regime under UN
control**

United Nations

Контроль над ИКТ-вооружениями

ICT Arms Control

1

Ограничение и/или отказ от наступательных ИКТ-возможностей для повышения ИКТ-стабильности

1

Limitation and/or rejection of offensive ICT opportunities for increase of ICT stability

2

Контроль за распространением ИКТ-возможностей

2

Control of ICT capabilities proliferation

3

Адаптация международного права к ИКТ-среде

3

Adaptation of international law to the ICT environment

СПАСИБО ЗА ВНИМАНИЕ!

**THANKS FOR YOUR
ATTENTION!**