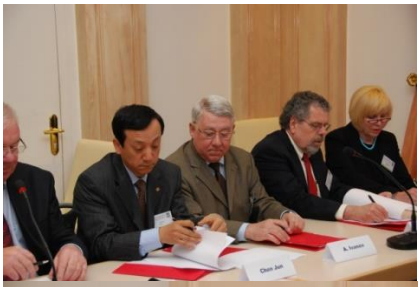
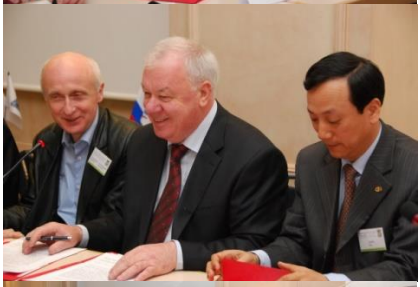
Международный исследовательский консорциум информационной безопасности (МИКИБ)

# Международный исследовательский консорциум информационной безопасности образован по инициативе Института проблем информационной безопасности МГУ имени М.В.Ломоносова 25 апреля 2010 года





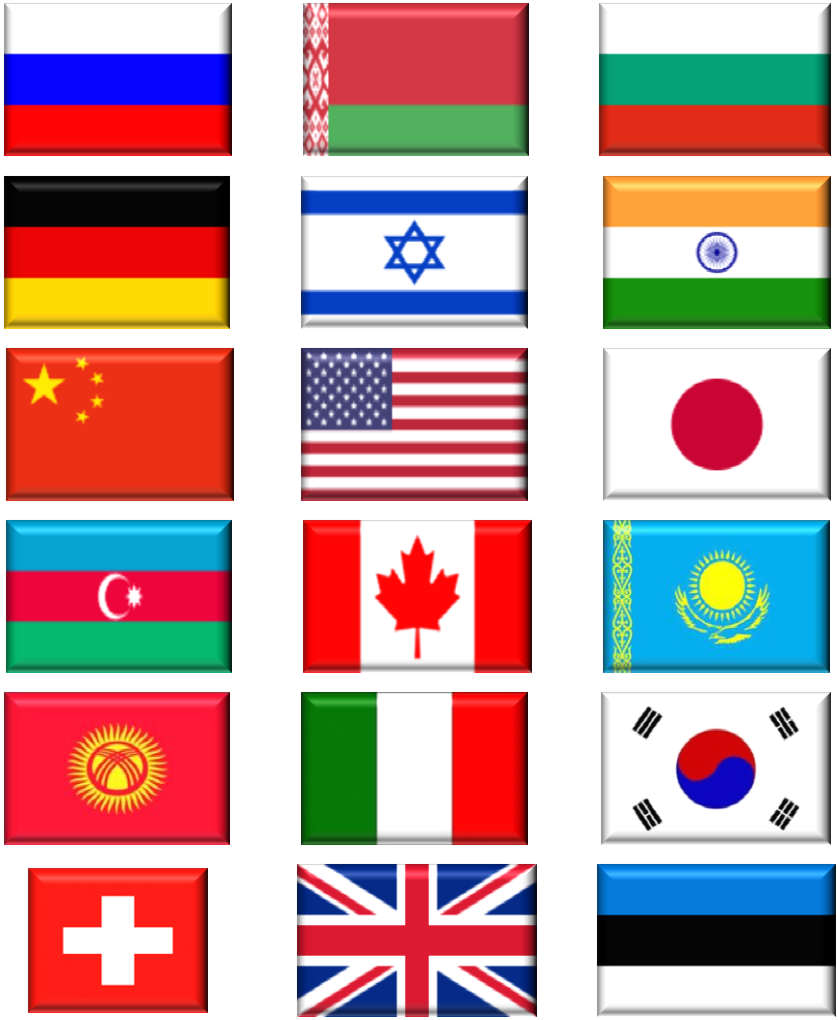
Церемония подписания декларации о создании МИКИБ (Германия, г. Гармиш-Партенкирхен)

Первоначально в МИКИБ вошли **11** организаций из **9** стран

На данный момент в состав МИКИБ входит **28** организаций из **18** стран

Международный исследовательский консорциум информационной безопасности (МИКИБ)

По состоянию на апрель 2019 года в МИКИБ входят **28** организаций из **18** стран



## Перечень организаций – учредителей МИКИБ

1. Институт проблем информационной безопасности МГУ имени М.В.Ломоносова
2. Объединенный институт проблем информатики Национальной Академии наук **Беларуси**
3. Интернет-сообщество **Болгарии**
4. Институт исследований вопросов киберпреступности (**Германия**)
5. Департамент информационной безопасности электронного правительства **Израиля**
6. **Индийский** институт информационных технологий в Аллахабаде
7. **Китайское** общество дружбы с зарубежными странами (КОДЗС)
8. Телекоммуникационная компания «МФИ Софт» (**Россия**)
9. Университет штата Нью-Йорк (**США**)
10. Компания «Глобал Сайбер Риск» (**США**)
11. Университет Токай (**Япония**)

## Перечень присоединившихся к МИКИБ организаций

12. Институт «Восток-Запад» (**США**)
13. Организация оборонных исследований и разработок Министерства обороны **Индии** (DRDO)
14. Хазарский Университет (**Азербайджан**)
15. Корпорация «PayPal» (**США**)
16. Фонд «SecDev» (**Канада**)
17. Университет «Кавказ» (**Азербайджан**)
18. Научно-исследовательский институт информационной безопасности и криптологии Евразийского национального Университета им. Л.Н.Гумилева (**Республика Казахстан**)
19. Институт электроники и телекоммуникаций при **Кыргызском** государственном техническом Университете им. И.Раззакова
20. Центр международной безопасности Университета Инсубрия (**Италия**)
21. Центр киберправа Университета Корё (**Республика Корея**)

22. Корпорация «ZTE» (**КНР**)
23. Фонд «ICT4Peace» (**Швейцария**)
24. ГМК «Норильский никель» (**Россия**)
25. Международный институт стратегических исследований (**Великобритания**)
26. Институт киберполитики (**Эстония**);
27. АО «Лаборатория Касперского» (**Россия**);
28. Редакция журнала «Международная жизнь» (**Россия**).

## Перечень приоритетных направлений и исследовательских проектов МИКИБ (утвержден в октябре 2010 года):

*Модели эскалации:* Разработка взаимоприемлемых моделей развития киберконфликтов, включая определения уровней враждебности

*Гражданские инфраструктуры:* Международный правовой статус гражданских киберинфраструктур в контексте войны и мира

*Определения:* Определения в области информационного противоборства и кибероборонs

*Киберзаконодательство:* Формы международного права для увеличения стабильности межгосударственных отношений и развития упорядоченных международных экономических процессов

*Кодексы поведения:* Развитие общеприемлемых норм поведения индивидов, государств и неправительственных организаций в киберпространстве

*Кибертерроризм:* Международные соглашения по противодействию негосударственным структурам, пытающимся провести кибератаки на государства или

спровоцировать конфликт между странами с использованием киберсредств

*Киберпреступность:* Законодательное и техническое взаимодействие в борьбе с киберпреступлениями

*Техническое сотрудничество:* Международная взаимная помощь в общественной и частной сферах по улучшению осведомленности о ситуации в киберпространстве, усилению защиты критически важных инфраструктур и реагированию на значительные кибераварии или атаки

*Защита сообществ:* Формы разделения технических элементов киберпространства (архитектура, функционирование) от экономических и политических вопросов и разработка отдельных механизмов для технической сферы и для политико-экономического уровня разрешения противоречий и выстраивания международного сотрудничества

*Промышленный шпионаж:* Форма международного права по промышленному шпионажу, спонсируемому государствами, и по вопросам продажи государствами результатов промышленного шпионажа на криминальном черном рынке

**На настоящий момент перечень дополнен следующими приоритетными направлениями:**

Адаптация международного права к конфликтам в информационном пространстве

Обеспечение информационной безопасности критически важных инфраструктур

Правила ответственного поведения государств в информационном пространстве

Обеспечение безопасности критически важных объектов информационной инфраструктуры

Формирование международной системы мониторинга угроз международной информационной безопасности

Противодействие использованию ИКТ для вмешательства во внутренние дела независимых государств

Правила ответственного поведения бизнеса в киберпространстве

Проблемы использования ИКТ в военно-политических целях

Разработка прогнозов и аналитических моделей развития Интернета

Безопасность, стабильность и отказоустойчивость глобальной инфраструктуры сети Интернет

**Решение**
**12-го международного форума «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности» и 16-й научной конференции Международного исследовательского консорциума информационной безопасности**
**16-19 апреля 2018 г., Гармиш-Партенкирхен, Германия**

1. Участники мероприятий на прошедших сессиях обсудили следующие актуальные проблемы международной информационной безопасности:

- Актуальные проблемы информационной безопасности в контексте развития цифровой экономики (семинар-круглый стол № 1);
- Механизмы реализации государственно-частного партнерства в области обеспечения безопасности критической информационной инфраструктуры (семинар-круглый стол № 2);
- Проблемы противодействия использованию ИКТ во враждебных военно-политических целях (семинар-круглый стол № 3);
- Механизмы выполнения норм, правил или принципов ответственного поведения

государств в ИКТ-среде (семинар-круглый стол № 4);

- Проблемы обеспечения «цифрового суверенитета» государств (семинар-круглый стол № 5);
- Предложения по новым проектам Международного исследовательского консорциума информационной безопасности в области международной информационной безопасности (16-я Конференция МИКИБ).

2. В рамках семинара-круглого стола № 1 участники обсудили следующие вопросы:

- Проблемы международного сотрудничества при развитии цифровой экономики.
- Цифровизация экономики и обеспечение информационной безопасности.

По итогам обсуждений эксперты пришли к выводу, что развитию цифровой экономики нет альтернативы, она обладает большой инвестиционной привлекательностью, но инвесторы слабо представляют себе угрозы информационной безопасности и не готовы вкладывать ресурсы в её обеспечение.

3. В рамках семинара-круглого стола № 2 участники обсудили следующие вопросы:

- Последние инициативы частного бизнеса в области обеспечения безопасности критической информационной

инфраструктуры. Как нам объединить наши усилия?

- Практика нормативно-правового регулирования вопросов обеспечения информационной безопасности, включая обмен опытом по выстраиванию механизмов взаимодействия CERT-ов различных форм собственности и в различных юрисдикциях.
- Проблемы, угрозы и вызовы монополизма поставщиков IT- систем и решений в области информационной безопасности по отдельным направлениям. Протекционизм и защита отечественных рынков против свободы торговли и предпринимательства.

Эксперты подробно обсудили состояние дел с реализацией государственно-частного партнерства в разных странах по обеспечению безопасности критической информационной инфраструктуры. Был отмечен определенный прогресс в этой области за последние годы, но вместе с тем и значительное отставание принимаемых мер от стремительно растущих количественно и качественно киберугроз, в частности, отмечались некоторые проблемы разделения ролей государства и бизнеса при обеспечении безопасности критической информационной инфраструктуры. В этой связи все эксперты поддержали инициативы ГМК

«Норильский никель» и корпорации Microsoft, содержащиеся в «Хартии информационной безопасности критических объектов промышленности» и «Цифровой Женевской Конвенции».

4. В рамках семинара-круглого стола № 3 участники обсудили следующие вопросы:

- Количественное и качественное расширение ИКТ-угроз в военно-политической сфере.
- Возможные меры по предотвращению или ограничению опасной деятельности в информационном пространстве.
- Определение мер укрепления доверия и сдерживания для предотвращения случайной эскалации конфликта в киберпространстве.

Эксперты согласились с тем, что необходимо в рамках Гармиш-процесса продолжить дискуссии по тематике противодействия использованию ИКТ во враждебных политических целях, имея в виду, в первую очередь, меры по предотвращению кибервойны. По итогам обсуждений эксперты пришли также к следующим выводам:

- проблемы применения международного права для предотвращения конфликтов в киберпространстве остаются весьма актуальными; среди них наиболее сложными являются: проблема атрибуции, проблема

фиксации юридических фактов враждебного использования ИКТ и проблема определения причинно-следственных связей между киберинцидентом и возможными последствиями его реализации;
- враждебное использование ИКТ способно стать фактором воздействия на стратегическую стабильность.

5. В рамках семинара-круглого стола № 4 участники обсудили следующие вопросы:
- Какие проблемы неоднозначного толкования и применимости выявлены в конкретных пунктах правил, вошедших в доклад ГПЭ 2015 года?
- Возможно ли разработать Руководство по применению правил, указанных в п.1?

По итогам обсуждений эксперты пришли к выводу, что в сложившейся ситуации ускоренного массового освоения киберпространства самыми различными акторами оставлять его без правил – значит создать хаос с непредсказуемыми последствиями. Реальной основой таких правил могут быть только «Рекомендации по нормам, правилам или принципам ответственного поведения государств в ИКТ-среде», вошедшие в доклад ГПЭ ООН 2015 г. В этой связи необходимо направить усилия экспертного сообщества на разработку согласованных процедур и

механизмов выполнения указанных правил, не дожидаясь закрепления их окончательной редакции на уровне ООН.

6. В рамках семинара-круглого стола № 5 участники обсудили следующие вопросы:

- Как обеспечить режим «цифровой границы»? (что такое режим и его основные функции; технологические проблемы; возможные технические решения; экономика границы).
- Как договариваться о «цифровой границе»? (условия для соглашений; предмет соглашений о границе; предмет соглашений о режиме границы).
- Цифровое пространство и границы в будущем. (BGP, SDN, IPv6; географическое распределение адресов и географическая маршрутизация; адрес как атрибут для режима границы (паспорт\виза); маркировка потоков информации и управление ими).

По итогам обсуждений эксперты пришли к выводу, что в настоящее время с технологической точки зрения провести «цифровую границу» вполне реально. С позиций обеспечения «цифрового суверенитета» государств остаются политические и юридические вопросы: принятие решения о целесообразности установления режима «цифровой границы» и придание этому режиму международно-правового статуса в какой-либо

форме (односторонний акт, двухстороннее или многостороннее соглашение).

7. На 16-й конференции МИКИБ участники, с учетом результатов работы семинара-круглого стола № 4, обсудили вопрос об организации работ по новому проекту МИКИБ, связанному с применением правил ответственного поведения государств в ИКТ-среде. Было принято решение создать дирекцию проекта в следующем составе:

- А.А.Стрельцов, ИПИБ МГУ;
- Андреас Кюн (Andreas Kuehn), Институт Восток-Запад, США;
- Энекен Тикк (Eneken Tikk), Институт киберполитики, Эстония;
- Ноюн Пак (Nohyoung Park), Центр киберправа Университета Корё, Республика Корея;
- Дэниел Штауффахер (Daniel Stauffacher), Фонд ICT4Peace, Швейцария.

## Конференции МИКИБ

ФРГ
апрель 2010

Россия
октябрь 2010

ФРГ
апрель 2011

КНР
октябрь 2011

ФРГ
апрель 2012

Болгария
октябрь 2012

ФРГ
апрель 2013

Азербайджан
октябрь 2013

ФРГ
апрель 2014

Казахстан
октябрь 2014

ФРГ
апрель 2015

Респ. Корея
ноябрь 2015

ФРГ
апрель 2016

ФРГ
апрель 2017

Россия
декабрь 2017

ФРГ
апрель 2018

Россия
декабрь 2018