ПРОГРАММА

Десятого международного форума «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности»

и

Тринадцатой научной конференции Международного исследовательского консорциума информационной безопасности

25–28 апреля 2016 года

Гармиш-Партенкирхен, Германия

Atlas Posthotel

25 апреля 2016 года, понедельник

09.00-10.00 **Регистрация участников**

10.00-13.00 **Открытие Конференции**
Пленарное заседание

1. **Шерстюк В.П.**, Сопредседатель оргкомитета Форума, советник Секретаря Совета Безопасности Российской Федерации, директор Института проблем информационной безопасности МГУ имени М.В.Ломоносова
2. **Крутских А.В.,** Специальный представитель Президента Российской Федерации по вопросам международного сотрудничества в области информационной безопасности
3. **Дылевский И.Н.,** Министерство обороны Российской Федерации

11.30-12.00 Кофе-брейк

4. **Солдатов А.А.,** Председатель Совета Фонда развития Интернет, Россия
5. **Якушев М.В.**, Вице-президент ICANN по Восточной Европе и Средней Азии
6. **Гасумянов В.И.,** Вице-президент – руководитель Блока корпоративной защиты, Норильский никель, Россия

13.00-18.00

Семинар – круглый стол № 1
Толкование основных понятий, принципов и норм Женевских конвенций применительно к киберпространству

Ведущие:
- **Стрельцов А.А.,** Институт проблем информационной безопасности МГУ имени М.В.Ломоносова
- **Энекен Тикк-Рингас (E.Tikk-Ringas),** Международный Институт Стратегических Исследований (Великобритания)

Вопросы, выносимые на обсуждение:

1. ИКТ как средство ведения военных действий
2. Атрибуция субъектов вооруженных конфликтов в сфере ИКТ
3. Обозначение объектов и субъектов сферы ИКТ, защищаемых международным гуманитарным правом
4. Комбатанты в вооруженных конфликтах в сфере ИКТ
5. Права человека в ходе вооруженных конфликтов в сфере ИКТ

Доклады:

1. **Стрельцов А.А.,** Институт проблем информационной безопасности МГУ имени М.В.Ломоносова
2. **Энекен Тикк-Рингас (E.Tikk-Ringas),** Международный Институт Стратегических Исследований (Великобритания)

14.00-15.30 – обед

3. **Уильям Бутби (William Boothby)** Женевский центр по вопросам политики безопасности (Великобритания)
   Подходы к применению права в киберпространстве – личный взгляд

4. **Пилюгин П.Л.,** Институт проблем информационной безопасности МГУ имени М.В.Ломоносова
   Проблемы опознавания объектов в киберпространстве

5. **Джон Мэллори (John Mallery)** Массачусетский технологический институт (MIT), США
   Итоги конференции Кибер нормы 4.0

26 апреля 2016 года, вторник

9.00-11.30

Семинар – круглый стол № 2
Проблемы нераспространения кибероружия и уменьшения опасности его использования

Ведущие:

- **Ященко В.В.,** Институт проблем информационной безопасности МГУ имени М.В.Ломоносова
- **Найджел Инкстер (Nigel Inkster)** Международный Институт Стратегических Исследований (Великобритания)
- **Хань Бяо (Han Biao),** Оборонный научно-технический университет НОАК, КНР

Вопросы, выносимые на обсуждение:

1. Содержание понятий «информационное оружие» и «кибероружие»
2. Методология выработки согласованных определений и концепций военных кибервозможностей и военных кибероперациий как один из инструментов укрепления доверия
3. Вассенаарские договоренности как элемент режима нераспространения информационного оружия
4. Возможные принципы построения режима нераспространения информационного оружия
5. Система международной информационной безопасности как средство предотвращения военных конфликтов, которые могут возникнуть в результате агрессивного применения информационного оружия

Доклады:

1. **Ященко В.В.,** Институт проблем информационной безопасности МГУ имени М.В.Ломоносова
2. **Найджел Инкстер (Nigel Inkster)** Международный институт стратегических исследований (Великобритания)
3. **Хань Бяо (Han Biao),** Оборонный научно-технический университет НОАК, КНР
4. **Уильям Бутби (William Boothby)** Женевский центр по вопросам политики безопасности (Великобритания)
   Возможные подходы к определению боевого кибероружия и его применения
5. **Майкл Сулмейер (Michael Sulmeyer),** Белферовский центр по науке и международным отношениям при факультете государственного управления им. Кеннеди Гарвардского университета
   Идеи об управлении эскалацией кризиса в киберпространстве
6. **Тим Маурер (Tim Maurer)** Фонд Карнеги за международный мир
   Частный рынок кибервозможностей

7. **Мика Керттунен (Mika Kerttunen),** Институт киберполитики, (Финляндия)
Сборник IISS «Military Balance» – методики сравнения военных кибервозможностей

8. **Маурицио Мартеллини (Maurizio Martellini),** Центр международной безопасности Университета Инсубрия (Италия), **Сандро Гайкен (Sandro Gaycken),** Европейская школа менеджмента и технологий (Германия), **Клэй Уилсон (Clay Wilson),** Система Американских государственных университетов (США)
Актуальные вопросы возможных военных аспектов кибервойны

11.30-12.00 Кофе-брейк

12.00-18.30 **Круглый стол «Проблемы современных международных отношений в контексте киберпространства»**

Ведущий:
Смирнов А.И., Президент Национального института исследований глобальной безопасности (НИИГлоБ), Чрезвычайный и Полномочный Посланник Российской Федерации

Вопросы, выносимые на обсуждение:

1. Государственный суверенитет в киберпространстве

2. Правила ответственного поведения государств в ИКТ-среде

3. Международная уполномоченность и ответственность за обеспечение устойчивости, надежности и безопасности Интернета

В дискуссии принимают участие:

Крутских А.В., Специальный представитель Президента Российской Федерации по вопросам международного сотрудничества в области информационной безопасности

Стрельцов А.А., Институт проблем информационной безопасности МГУ имени М.В.Ломоносова

Сандро Гайкен (Sandro Gaycken), Европейская школа менеджмента и технологий, Германия

Энекен Тикк-Рингас (E.Tikk-Ringas), Международный Институт Стратегических Исследований (Великобритания)

Хань Бяо (Han Biao), Национальный университет оборонных технологий КНР

Ноюнг Пак (Nohyoung Park), Центр киберправа Университета Корё (Республика Корея)

Дэниел Штауффахер (Daniel Stauffacher), фонд ICT4Peace (Швейцария)

Найджел Инкстер (Nigel Inkster) Международный Институт Стратегических Исследований (Великобритания)

Джон Мэллори (John Mallery) Массачусетский технологический институт (MIT), США

Рафал Рогозински (Rafal Rohosinski), SecDev, Канада

Якушев М.В., ICANN

14.00-15.30 – обед

Доклады:

1. **Смирнов А.И.,** Национальный институт исследований глобальной безопасности, Россия
   Четвертая промышленная революция: информационные риски – взгляд из России
2. **Бен Хиллер (Ben Hiller),** ОБСЕ
   Выстраивание мер доверия между государствами и нормы ответственного поведения государств в киберпространстве: две стороны одной медали
3. **Уильям Бутби (William Boothby)** Женевский центр по вопросам политики безопасности (Великобритания)
   Диалог между военными по использованию кибероружия, как отдельная мера укрепления доверия
4. **Санджай Гоел (Sanjay Goel)**, Университет штата Нью-Йорк (США)
   Суверенитет и Интернет
5. **Фил Гурски (Phil Gurski),** SecDev, Канада
   Что делать с использованием социальных сетей террористами?
6. **Поляков М.Л.,** Московский государственный институт международных отношений, Россия
   Новые медиа и киберпространство: современные способы производства и распространения информации
7. **Джон Мэллори (John Mallery)** Массачусетский технологический институт (MIT), США
   Динамика эскалации в информационном конфликте

27 апреля 2016 года, среда

9.00-11.30

Семинар – круглый стол № 3
Механизмы и инструменты частно-государственного партнерства в области обеспечения информационной безопасности критически важных объектов

Ведущие:

- **Кульпин А.А.,** Норильский никель, Россия
- **Сандро Гайкен (Sandro Gaycken),** Институт цифрового общества, Европейская школа менеджмента и технологий, Германия

Вопросы, выносимые на обсуждение:

1. **Обмен информацией:** Что представляет собой серьезный инцидент в критически важной информационной инфраструктуре и как следует сообщать о нем? Необходимо ли также сообщать о низкоуровневом вторжении, принимая во внимание потенциал его развития в инцидент высокого уровня? Нужно ли в случае с инцидентами, которые обладают потенциальным международным влиянием, сообщать о них на международном уровне?
2. **Планы развития технологий и инвестиции:** Какие перспективные технологии необходимо разрабатывать, и каким должно быть взаимодействие промышленности и государства по созданию новых компаний IT-безопасности, призванных реализовать эти технологии? Где можно привлечь инвестиции в кибербезопасность, и как инвесторы могут быть уверены, что инвестируют в правильный продукт? Как государство может помочь продавать продукцию? Какова роль доверия в области ИТ-экспорта, и как она влияет на создание и развитие компаний?
3. **Безопасность цепи поставок**: Насколько уязвимы цепи поставок, и какие это несёт риски для критически важной информационной инфраструктуры? Как можно их контролировать? Кто должен разрабатывать и реализовывать технологии, нужные для обеспечения безопасности цепи поставок? Должны ли они регулироваться так же жестко, как и критически важная информационная инфраструктура?
4. **Баланс регулирования:** Насколько жестко и в каких областях должны регулироваться инфраструктуры? Каким должно быть разумное регулирование, и что должен знать регулятор, чтобы предложить хорошие законы? Как промышленность может продуктивным образом участвовать в регулировании?
5. **Международное частное сотрудничество:** Как следует регулировать международное частное сотрудничество в области кибербезопасности? Какой информацией и технологиями можно обмениваться? Насколько полезно сотрудничество между многонациональными компаниями различного происхождения?

Доклады:

1. **Кульпин А.А.,** Норильский никель, Россия
2. **Сандро Гайкен (Sandro Gaycken),** Европейская школа менеджмента и технологий, Германия

3. **Ярных А.Ю.,** Лаборатория Касперского
Уязвимость критически важной инфраструктуры, итоги 2015 года

4. **Рольф Райнема (Rolf Reinema),** Siemens **(тема уточняется)**

5. **Чарльз Барри (Charles Barry)** Институт национальной стратегии, Университет национальной обороны США
Стратегические аспекты защиты критически важной информационной инфраструктуры

6. **Баранов А.П.,** Национальный исследовательский университет «Высшая школа экономики», Россия
Информационная безопасность массовых компьютерных систем

7. **Томас Ламанаускас (Tomas Lamanauskas),** Вымпелком (Европа)
Операторы связи как ключевые партнеры в защите критически важной инфраструктуры

11.30-12.00 Кофе-брейк

12.00-14.00

Тринадцатая научная конференция Международного исследовательского консорциума информационной безопасности (МИКИБ)

Ведущий:
Шерстюк В.П., Руководитель-организатор Международного исследовательского консорциума информационной безопасности, советник Секретаря Совета Безопасности Российской Федерации, директор Института проблем информационной безопасности МГУ имени М.В.Ломоносова

Доклады о проектах МИКИБ:

1. **Медриш М.А.,** Фонд поддержки Интернет

2. **Стрельцов А.А.,** Институт проблем информационной безопасности МГУ имени М.В.Ломоносова

3. **Ержан Сейткулов,** НИИ информационной безопасности и криптологии Евразийского национального университета им. Л.Н.Гумилева, Казахстан

4. **Рафал Рогозински (Rafal Rohosinski),** SecDev, Канада, **Найджел Инкстер (Nigel Inkster)** Международный Институт Стратегических Исследований (Великобритания)

Организационные вопросы:

5. Принятие решения о теме, программе, времени и месте проведения Четырнадцатой научной Конференции МИКИБ

14.00-15.30 – обед

15.30-18.00

Семинар – круглый стол № 4
Меры противодействия Интернет-рекрутингу и Интернет-пропаганде экстремизма и терроризма

Ведущие:

- Шаряпов Р.А., Институт проблем информационной безопасности МГУ имени М.В.Ломоносова

- Ноюнг Пак (Nohyoung Park), Центр киберправа Университета Корё, Республика Корея

- Рафал Рогозински (Rafal Rohosinski), SecDev, Канада

Вопросы, выносимые на обсуждение:

1. Возможные международно-правовые и политические инициативы противодействия Интернет-рекрутингу и Интернет-пропаганде экстремизма и терроризма, в особенности установление механизма ответственности хостинг-провайдеров в рамках межгосударственного сотрудничества и частно-государственного партнерства за поддержку экстремистских и террористических сайтов
2. Лучшие национальные гуманитарные практики противодействия Интернет-рекрутингу и Интернет-пропаганде экстремизма и терроризма
3. Проблемы научно-технологического обеспечения работ по выявлению деструктивного контента и его источников

Доклады:

1. **Шаряпов Р.А.,** Институт проблем информационной безопасности МГУ имени М.В.Ломоносова
2. **Ноюнг Пак (Nohyoung Park),** Центр киберправа Университета Корё, Республика Корея
3. **Рафал Рогозински (Rafal Rohosinski),** SecDev, Канада
4. **Масалович А.И.,** ДиалогНаука, Россия
   Выявление признаков пропаганды экстремизма в Сети. Анализ социальных портретов экстремистов, вербовщиков и их потенциальных жертв.
5. **Ромашкина Н.П.,** Институт мировой экономики и международных отношений имени Е.М.Примакова Российской академии наук
   Противодействие угрозам в киберпространстве: роль научных и образовательных учреждений

28 апреля 2016 года, четверг

Двусторонние и многосторонние переговоры и консультации

(по договоренности)