Меры доверия в сфере Международной информационной безопасности

И.Е. Костунов

Угрозы в сфере использования ИКТ и самих ИКТ являются одной из наиболее серьезных проблем, с которыми человечество сталкивается на современном этапе.

Совместное заявление президентов Российской Федерации и США о новой области сотрудничества в укреплении доверия (17.06.2013)

Меры доверия

- любые мероприятия, направленные на укрепление взаимопонимания и доверия между государствами
- действия в военной, политической и дипломатической сферах, нацеленные на снижение уровня напряженности в межгосударственных отношениях, которая может привести к возникновению военного конфликта.

Дилемма безопасности

- попытки государств повысить собственную безопасность, вне зависимости от их намерений, приводит к снижению безопасности других государства, в силу того, что каждый игрок интерпретирует свои шаги как оборонительные, а действия остальных — как потенциально наступательные

Политический реализм

мотивы поведения государств:

- стремление максимизировать собственную безопасность
- приобрести как можно больше ресурсов в условиях анархичной и высококонкурентной внешней среды
- государства являются единственными значимыми игроками.

Политический конструктивизм

мотивы поведения государств:

- Не «материалистические соображения», а «социальные конструкты»
- Ощущение страха, культурные мотивы и другие элементы социальной реальности
- Идентичность и интересы акторов создаются под влиянием идей, а не их природой.

Типы и содержание МД в военной сфере

Тип МД	Содержание МД
1) **уведомление** об отдельных видах военной деятельности, которая может быть расценена как провокационная	- предварительное информирование об учениях, маневрах, включая перемещение войсковых группировок - информирование о значительных изменения в размерах подразделений, их вооружении и задачах
2) **наблюдение** за отдельными видами военной деятельности, которая может быть расценена как провокационная	- направление наблюдателей на учения - назначение постоянных наблюдателей при штабах национальных вооруженных сил - авиационные облеты
3) **обмен информацией**	- опасные инциденты
4) **повышение транспарентности**	информирование о: - военном бюджете - элементах военной доктрины - расположении подразделений - новых типах вооружений - крупных изменениях в данных параметрах

Типы и содержание МД в военной сфере

Тип МД	Содержание МД
5) **контакты**	- консультации - визиты делегаций - обмен учащимися и преподавателями военных учебных заведений - повышение квалификации иностранных военнослужащих - назначение военных атташе
6) **повышение осведомленности**	- создание общедоступного и открытого реестра (под эгидой международной организации), перечня, базы данных для сбора информации о вооружениях государств-участников
7) **сотрудничество**	- совместные учения - создание демилитаризованных зон в приграничных территориях - совместное патрулирование приграничных территорий

Вероятность принятия МД

1) наличие двух либо нескольких ключевых игроков (государств или блоков), имеющих равные либо сопоставимые военные возможности;

2) наличие у них внешнеполитической доктрины, ориентированной вовне (экспансивной);

3) наличие между данными игроками существенных идеологических противоречий, которые поддерживают стабильно высокий уровень недоверия между ними;

4) готовность (политическая воля) руководства данных государств или блоков к использованию технологических преимуществ в наступательных целях.

Отличие ИКТ от обычных вооружений

- низкая стоимость по сравнению с ядерными и обычными вооружениями
- техническая доступность и относительная простота эксплуатации
- необязательно иметь постоянный штат сотрудников: в мире сложился глобальный теневой рынок хакерских услуг
- точность и избирательность действия, которую не способны обеспечить традиционные виды вооружений

Сравнительная характеристика «традиционных» МД в военной области (на примере ОБСЕ) и МД в сфере использования ИКТ

	МД в военной области	**МД в сфере использования ИКТ**
Статус соглашений о МД	Юридически обязывающие	Российско-американские двусторонние договоренности – юридически обязывающие (в форме приложений к действующим соглашениям)
Характер МД	Политически обязательные	Добровольные
Субъект международно-правового регулирования в рамках МД	Государство	Государство
Фактический субъект МД	Государство	Государство и негосударственные игроки (хакерские и другие криминальные группировки, террористические организации, отдельные граждане)
Участники реализации МД	Государство	Государство, обсуждается привлечение бизнес-структур, НПО, научных кругов
Объект МД	- материальные объекты (личный состав, системы вооружений и военная техника) - нематериальные объекты (военная доктрина, планы военного строительства, бюджет, характеристики вооружения; информация в отношении опасных инцидентов военного характера)	(в стадии формулирования) - материальные объекты (критическая инфраструктура, функционирование которой обеспечивается ИКТ) - нематериальные объекты (доктрина в области информационной безопасности, подходы к классификации угроз и инцидентов в сфере использование ИКТ; информация о компьютерных инцидентах и необычной активности в сети Интернет)

Сравнительная характеристика «традиционных» МД в военной области (на примере ОБСЕ) и МД в сфере использования ИКТ

	МД в военной области	МД в сфере использования ИКТ
Принципы реализации МД	- соответствие общепризнанным принципам международного права - добровольность - равная безопасность участников - непричинение ущерба безопасности третьих стран	(в стадии формулирования) - соответствие общепризнанным принципам международного права - добровольность
Механизм верификации выполнения МД	Инспекции на местах, посещение военных объектов, наблюдательные авиационные облеты, национальные технические средства контроля	(в стадии формулирования)
Характер отчетности о реализации МД	Жесткая: государство обязано отчитаться о ходе реализации МД и дать разъяснения в случае невыполнения, в том числе сообщить причину и уведомить о дате планируемого выполнения	(в стадии формулирования) В ОБСЕ: Отчетность не предусмотрена, для обсуждения хода реализации МД и возможности выработки новых МД проводятся регулярные встречи на экспертном уровне
Механизм представления отчетности о реализации МД	Ежегодное совещание государств-участников по оценке выполнения МД, проводится Форумом по сотрудничеству в области безопасности	

Применимость и целесообразность отдельных типов МД в сфере использования ИКТ

Тип МД	Содержание МД	Техническая применимость МД в сфере использования ИКТ	Целесообразность реализации
(1) меры немедленного реагирования	линии прямой связи на высоком политическом уровне	Применимы	Высокая
	каналы обмена информацией об опасных инцидентах		
(1) меры повышения предсказуемости	уведомление об отдельных типах военной деятельности (учениях, маневрах, крупные перемещения войск)		Низкая
(1) меры транспарентности	обмен информацией о военных доктринах		Средняя
	обмен информацией о военном бюджете		Нецелесообразно
	обмен информацией о расположении подразделений		
	обмен информацией о новых типах вооружений		
(1) меры стабилизации	пороговые уровни вооружений и военной техники	Неприменимы	----------

Применимость и целесообразность отдельных типов МД в сфере использования ИКТ

Тип МД	Содержание МД	Техническая применимость МД в сфере использования ИКТ	Целесообразность реализации
(1) меры сотрудничества	совместные учения, постоянно действующие контактные группы, рабочие группы экспертов	Применимы	Высокая (исключая совместные учения)
(1) меры повышения осведомленности	тематические базы данных, перечни, глоссарии		Средняя
(1) контакты на экспертном уровне	консультации, иные визиты делегаций, обмен преподавателями и учащимися, программы повышения квалификации		Высокая
(1) дискуссионные площадки	семинары, круглые столы, конференции		Средняя

Основные документы РФ, где отображена позиция по безопасности в сфере ИКТ

- Доктрина ИБ РФ (9.09.2000)
- Военные доктрины (2010, 2014)
- Стратегия развития информационного общества в РФ (7.02.2008)
- Основные направления государственной политики в области обеспечения безопасности АСУ производственными и технологическими процессами критически важных объектов инфраструктуры РФ (03.02.2012)
- Основы государственной политики РФ в области МИБ на период до 2020 года (06.2013)
- Стратегия национальной безопасности РФ (31.12.2015)

Проект Конвенции ООН об обеспечении международной ИБ

- Обмен национальными концепциями ИБ
- Оперативный обмен данными о кризисных событиях и угрозах в информационном пространстве, и принимаемых мерах
- Проведение консультаций по вопросам деятельности в информационном пространстве, которая может вызвать озабоченность
- Сотрудничество в отношении урегулирования военных конфликтов.

Положение о необходимости выработки МД в сфере использования ИКТ включено в межправительственное соглашение о сотрудничестве в области обеспечения МИБ, между РФ и США, между РФ и Китаем, между РФ и Белоруссией.

Правила поведения в области обеспечения МИБ

- Концепция на предотвращение конфликтов в информационной сфере через мягкие правила.
- Уважение государственного суверенитета
- Невмешательство во внутренние дела других государств
- Основные права человека
- Равные права для всех государств на участие в управлении сетью Интернет.

Российско-американские договоренности об укреплении доверия в сфере использования ИКТ

Название документа	статус	Ведомства ответственные за реализацию	Цель
1) Совместное заявление президентов Российской Федерации и США о новой области сотрудничества в укреплении доверия (17.06.2013)	Политическая декларация	Все компетентные ведомства, занимающиеся вопросами ИБ	Укрепление взаимопонимания в сфере использования ИКТ. Установление регулярного межведомственного диалога по вопросам угроз в сфере ИКТ и самим ИКТ путем создания двусторонней рабочей группы
1) Соглашение об организации линии прямой шифрованной связи между уполномоченными представителями США и России по вопросам угроз в сфере использования ИКТ и самим ИКТ	Межправительственное соглашение.	От РФ – ФСО От США – Агентство информационных систем МО США.	Создание канала оперативной коммуникации между лицами непосредственно координирующими деятельность компетентных ведомств в вопросах связанных с обеспечением ИБ

Российско-американские договоренности об укреплении доверия в сфере использования ИКТ

Название документа	статус	Ведомства ответственные за реализацию	Цель
Протокол об обмене уведомлениями о деятельности несущей угрозу для информационно-коммуникационных сетей, систем или инфраструктуры	Межгосударственный протокол Протокол к межгосударственному Соглашению о создании Центров по уменьшению ядерной опасности (1987).	От РФ – НЦУЯО (в составе МО) От США – НЦУЯО (в составе Госдепартамента)	Обмен уведомлениями о деятельности в сети, которая может вызвать озабоченность другой стороны. (компьютерная угроза, учения в сфере ИКТ)
Приложение об обмене информацией об индикаторах вредоносной деятельности	Межведомственное Приложение к Меморандуму о взаимопонимании между Министерством внутренней безопасности США и ФСБ России(2006)	От РФ – ФСБ России (RUS-CERT) От США – МВБ США (US-CERT)	Организация обмена индикаторами вредоносной активности в сетях в целях повышения защищенности критически важных информационных систем

Выводы

«автоматическое» распространение модели МД, сложившейся в военной сфере в реальном (физическом) мире, на цифровую сферу невозможно:

1. технологические ограничения
2. международно-правовые лакуны в регулировании этой сферы, в том числе в рамках института МД
3. необходим тщательный отбор тех типов МД, которые не нарушают баланс между укреплением доверия между государствами и интересами национальной безопасности

Выводы

Для внедрения МД, в цифровую сферу необходимо:

1. Технологические стандарты безопасности, прогнозирование и контроль опасностей и угроз на ранней стадии
2. Развитие международно-правового обеспечения этой сферы, в том числе в рамках института МД
3. Добровольность МД в ИКТ
4. Формирование баланса и актуализация взаимной неприемлемости ущерба от реализации угроз в сфере ИКТ.