О первостепенных задачах в сфере международной информационной безопасности

Уважаемые организаторы симпозиума!

Уважаемые участники!

Дамы и господа!

Коллеги!

1 ноября этого года ректор Московского университета академик Садовничий Виктор Антонович принял участие в торжествах по случаю 75-летия Университета Токай. В 1942 году доктор Шигеоси Мацумаэ основал это уникальное учебное заведение, с которым Московский Университет сотрудничает с 1973 года.

Наша делегация от лица Института проблем информационной безопасности МГУ им. М.В. Ломоносова поздравляет студентов, аспирантов, преподавателей, трудовой коллектив и руководителей Университета Токай с замечательным юбилеем! Мы благодарны ректору Университета господину Киёси Ямада за приглашение принять участие в Симпозиуме по развитию современных тенденций в области обеспечения международной информационной безопасности.

В следующем году исполняется 20 лет с того времени, как появился этот термин – международная информационная безопасность.

Начало данному процессу положило специальное послание министра иностранных дел России И.С. Иванова, направленное 23 сентября 1998 г. Генеральному секретарю ООН Кофи Аннану.

В принятой в 1999 г. резолюции Генеральной Ассамблеи ООН «Достижения в сфере информатизации и коммуникаций в контексте международной безопасности» впервые была сформулирована «триада угроз» в сфере международной информационной безопасности: применение

информационно-коммуникационных технологий (ИКТ) в военных, террористических и преступных целях.

Обсуждение проблем предупреждения негативных последствий применения ИКТ в контексте международной безопасности, разоружения и других областей, связанных с этим процессом, продолжается на сессиях Генеральной Ассамблеи ООН ежегодно.

Международное сообщество отмечает возрастание на современном этапе развития и внедрения информационных технологий и средств телекоммуникаций опасности использования этих технологий в целях нарушения международного мира. При этом особое внимание обращается на необходимость предотвращения межгосударственной конфронтации, способной спровоцировать новый виток гонки вооружений в информационной сфере.

По нашему мнению, одним из наиболее эффективных путей решения данных проблем является укрепление международной информационной безопасности.

Вопросам международной информационной безопасности были посвящены международные конференции и семинары, в том числе проведенные под эгидой Института ООН по проблемам разоружения и Международного комитета Красного Креста. По инициативе России на 56-й сессии Генассамблеи ООН 29 ноября 2001 года было принято принципиально важное решение о создании специальной группы правительственных экспертов для изучения проблемы международной информационной безопасности. В 2004 году такая группа была создана. В мандат группы вошло рассмотрение угроз в сфере информационной безопасности, возможных совместных мер по их устранению, а также проведение исследования концепций укрепления безопасности глобальных информационных и телекоммуникационных систем.

Исследовательские усилия Группы правительственных экспертов ООН позволили акцентировать внимание всех государств – членов Организации на

угрозах международной безопасности и миру, обусловленных возможностью злонамеренного или враждебного использования государствами ИКТ против территориальной неприкосновенности, политической независимости других государств. Внимание международного сообщества обращалось и на опасность использования ИКТ негосударственными образованиями для подготовки или совершения террористических актов, а также других преступных деяний.

Многолетние усилия экспертов в 2015 году были отмечены консенсусным принятием доклада Генеральному Секретарю ООН, который по многим параметрам можно назвать прорывным. В нем были сформулированы принципы ответственного поведения государств в ИКТ среде, а также рекомендации по мерам доверия.

Стороны договорились о нескольких ключевых вещах:

Во-первых – не легализовывать и не регулировать конфликты в информационном пространстве, а предотвращать использование ИКТ в военно-политических целях.

Во-вторых – отказаться во взаимных обвинениях в кибератаках, как это сейчас нередко происходит, без серьезных на то доказательств.

В-третьих – ИКТ должны использоваться исключительно в мирных целях.

В-четвертых – признана незаконной и вредоносной деятельность по внедрению закладок в IT продукцию.

В-пятых – группа подтвердила суверенное право государств распоряжаться информационно-коммуникационной инфраструктурой на своей территории и определять свою политику в сфере международной информационной безопасности.

К сожалению, группа, созданная в 2016 году, не сумела поддержать набранный темп и не смогла достичь консенсуса при подготовке итогового доклада, но это не должно останавливать дискуссию по ключевым вопросам международной информационной безопасности и, тем более, использоваться

в качестве повода для девальвации роли ООН и перевода обсуждения данной проблематики на региональный уровень или даже в двусторонний формат.

Можно констатировать, что развитие ИКТ, их использование в различных сферах деятельности не сделали мир безопасным и более комфортным для людей. Продолжает возрастать опасность враждебного использования ИКТ в целях силового разрешения международных споров по поддержанию деятельности международных террористических операций, совершению трансграничных нарушений корыстной направленности, нарушению прав и свобод человека. Становится трендом современной международной политики использование фейковых событий в качестве повода для нагнетания международной напряженности. Все более сложными и изощренными становятся компьютерные атаки, количество которых на критически важные объекты и инфраструктуры государственного управления, кредитно-финансовой сферы не уменьшается.

Секретарь Совета безопасности РФ Николай Патрушев сообщил, что в 2016 году количество кибератак на сайты госорганов увеличилось, было зафиксировано около 52 с половиной миллионов случаев, а в 2015 году их было 14,4. За один год произошло их трехкратное увеличение. По данным ФСБ России на январь 2017 года, за последние годы ущерб от хакерских атак по всему миру составил, по разным оценкам, от 300 млрд до 1 триллиона долларов. Эти потери составляют от 0,4 до 1,5 мирового ВВП и имеют тенденцию к неуклонному росту. Повышается риск враждебного использования ИКТ с целью нарушения работоспособности критически важных объектов и инфраструктуры со стороны международных террористических организаций, а также некоторых государств.

Реальные, виртуальные и фейковые события превращают информационную сферу в фантасмагорию и создают значительные неопределенности в политической жизни человека.

Доверие между государством, бизнесом и частным сектором в киберпространстве, информационной сфере в целом не может

рассматриваться как явление, независимое от политической, экономической и социальной сфер, международной жизни. Доверие никогда не появится, если не поддерживать международное сотрудничество и процессы обсуждения сложных проблем международной безопасности, надо стремиться к предотвращению международных конфликтов, в которых используется как традиционное, так и информационное оружие.

Значительную работу по формированию системы мер доверия Российская Федерация совместно с другими заинтересованными государствами проводит, используя площадку Организации по сотрудничеству и безопасности в Европе. В 2016 году Постоянный совет государств-участников ОБСЕ принял решение о разработке проекта комплекса мер укрепления доверия с целью повышения межгосударственного сотрудничества, транспарентности, предсказуемости и стабильности, уменьшения рисков ошибочного восприятия, предупреждения эскалации конфликтов, которые могут возникнуть в результате использования ИКТ. С участием заинтересованных государств создана неофициальная группа по мерам укрепления доверия в области кибербезопасности.

Усилиями заинтересованных государств, в том числе Российской Федерации, в международном экспертном сообществе, намечается понимание необходимости соблюдения международных обязательств, вытекающих из признанных государствами источников международного права: общих и специальных международных конвенций; международного обычая; общих принципов права, признанных цивилизованными народами; судебных решений.

Основными признаками, отличающими ИКТ-среду как пространство международных отношений от традиционных пространств реализации отношений суверенных государств (суши, моря, воздушного пространства и космоса), являются:

искусственный характер ИКТ-среды, образуемой совокупностью средств телекоммуникаций, вычислительной техники, программного обеспечения, функционирующих в системе глобальных цифровых идентификаторов, работоспособность которой поддерживается усилиями, прежде всего, негосударственных организаций, находящихся в различных юрисдикциях;

виртуальность процессов применения ИКТ, следствием которой является невозможность непосредственного наблюдения условий возникновения инцидентов в ИКТ-среде;

трудность определения источников инцидента в ИКТ-среде;

дестабилизирующие последствия злонамеренного или враждебного использования ИКТ против критически важной инфраструктуры общества, совершения террористических нападений на объекты ИКТ-среды и связанную с ИКТ инфраструктуру;

использование ИКТ террористическими организациями для вербовки сторонников, финансирования, обучения, подстрекательства и проведения терактов.

Следует признать угрозой международной информационной безопасности использование ИКТ для вмешательства во внутренние дела суверенных государств. О необходимости противодействия этой угрозе Россия и некоторые другие государства неоднократно заявляли, как на уровне двусторонних консультаций по проблемам информационной безопасности, так и на уровне Шанхайской организации сотрудничеств. Российская Федерация совместно с другими государствами дважды – в 2011 и в 2015 гг. вносила проекты соответствующих резолюций в ООН.

Сегодня в экспертном международном сообществе можно отметить расхождения относительно базовых принципов формирования системы международной информационной безопасности. Часть из них исходит из того, что информационное пространство уже стало новым театром военных действий и предлагает сконцентрировать усилия на регулировании

неизбежных, по их мнению, военно-политических конфликтов с использованием ИКТ. При этом утверждается, что механизмы регулирования должны основываться на безусловной применимости существующих норм международного права, которые создавались в доцифровую эпоху. Они не видят необходимости договариваться об установлении границ зон ответственности государств в ИКТ среде, о процедуре объективизации данных о нарушении международных обязательств государствами, о порядке расследования международных инцидентов в ИКТ среде на основе взаимодействия национальных Групп реагирования на инциденты информационной безопасности.

С учетом практической невозможности достоверного определения источников компьютерных атак мы считаем, что такой подход фактически легализует возможность проведения не только информационных, но и военных операций против неудобных государств.

Иной подход, который поддерживают российские эксперты, основан на недопущении милитаризации информационного пространства и невмешательстве во внутренние дела других государств, на безусловном признании цифрового суверенитета государств. Использование бездоказательных обвинений в совершении компьютерных атак в качестве инструмента политического давления мы считаем недопустимым.

Несмотря на вышеперечисленные расхождения в подходах, мы считаем, что нам всем следует сосредоточить усилия на предотвращении конфликтов в ИКТ среде и недопущении использования ИКТ для достижения военных целей, а также – на прогрессивном развитии международного права, на адаптации его к особенностям ИКТ среды как нового пространства международного сотрудничества.

А теперь предложения:

Отметим первостепенные, на наш взгляд, задачи в сфере международной информационной безопасности, на которых следовало бы сконцентрировать внимание международному научному и экспертному

сообществу:

1. Подготовка проекта Конвенции по обеспечению международной информационной безопасности, закрепляющей основные подходы к прогрессивному развитию международного права применительно к ИКТ-среде посредством принятия норм, уточняющих содержание международных обязательств государств в ИКТ-среде, процедуру выявления нарушений этих обязательств, определения субъектов, нарушивших международные обязательства, а также процедуры мирного разрешения международных споров, связанных с инцидентами в ИКТ-среде.

2. Подготовка проекта руководства по применению принципов, норм и правил ответственного поведения государств в ИКТ-среде.

3. Подготовка проекта Конвенции по противодействию информационной преступности.

4 Подготовка проектов дополнений к существующим международным договорам, уточняющих содержание международных обязательств в ИКТ-среде, и, прежде всего, в контексте предупреждения возникновения международных конфликтов и мирного разрешения международных споров.

5. Подготовка универсального международного договора о порядке отграничения зон ответственности государств в ИКТ-среде и правового закрепления границ этих зон ответственности (пространственных пределов суверенитета государств в ИКТ-среде).

6. Подготовка международных соглашений о порядке расследования международных инцидентов в ИКТ-среде на основе взаимодействия Национальных центров реагирования на опасные события в данной среде, а также порядка приписывания субъектам международного права ответственности за возникновение таких инцидентов.

7. Создание международного органа для рассмотрения международных споров по вопросам безопасности продуктов, реализующих функции ИКТ, а также по вопросам использования ИКТ для вмешательства во внутренние дела суверенных государств.

На наш взгляд, исследовательскую работу по перечисленным направлениям можно вести одновременно по нескольким направлениям.

Во-первых, в направлении развития двустороннего сотрудничества между заинтересованными государствами. Это сотрудничество можно было бы ориентировать на установление взаимодействия между органами государственной власти в целях:

противодействия совершению преступлений, подготовки и осуществлению террористических актов;

формирования подходов к практической отработке комплекса мер доверия, соответствующего уровню двусторонних отношений;

применения правил ответственного поведения государств в ИКТ-среде.

Вторым направлением сотрудничества может стать развитие региональных систем обеспечения международной информационной безопасности. В рамках этой работы важно разработать методы применения рекомендаций по мерам доверия и добровольных правил, принципов и норм ответственного поведения государств в ИКТ-среде с учётом международных обязательств, принятых на себя государствами в рамках региональных соглашений о взаимодействии.

Наконец, в качестве предложения, стоило бы рассмотреть целесообразность создания при одной из международных организаций или Комиссии международного права при Генеральной Ассамблее ООН специализированной рабочей группы по подготовке предложений по проектам международных договоров. В состав такой группы было бы важно включить юристов, инженеров и представителей силовых структур заинтересованных государств. Экспертизу проектов документов, подготовленных специализированной рабочей группой, могла бы осуществить Группа правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. Компромиссы по проектам документов можно было бы искать в формате двусторонних и многосторонних консультаций.

На наш взгляд, определенный вклад в решение сформулированных задач могли бы внести Московский Университет и Университет Токай, в том числе и в формате совместных исследований.

Такое взаимодействие способствовало бы продвижению международного сообщества к более безопасному миру в условиях формирования глобального информационного общества.

Спасибо за внимание.