

Информационная безопасность – важный компонент взаимодействия в рамках ШОС



В условиях роста онлайн-активности и нарастания киберугроз обеспечение информационной безопасности превратилось в важнейший компонент взаимодействия в рамках ШОС.

По состоянию на 1 августа 2022 года из 5,4 миллиардов глобальных пользователей Интернета на страны ШОС приходится более 2,1 миллиарда, что обуславливает необходимость выработки общих подходов по обеспечению международной информационной безопасности.

При этом государства-участники ШОС видят в активном развитии информационно-коммуникационных технологий не только риски, но в первую очередь преимущества экономического и социального развития. С учетом этого, стороны разрабатывают меры по укреплению практического сотрудничества в данной сфере.

По итогам заседания Совета глав государств-членов ШОС 10 июня 2018 года в г.Циндао (КНР) была подчеркнута важность развития и углубления взаимовыгодного сотрудничества, обмена знаниями, информацией и передовой практикой в области информационно-коммуникационных технологий, в том числе в сфере цифровой экономики. В целях реализации данной инициативы уже через год, 14 июня 2019 года была утверждена Концепция сотрудничества ШОС в сфере цифровизации и информационно-коммуникационных технологий.

Среди приоритетных направлений реализации Концепции значились цифровая телекоммуникационная инфраструктура, информационная безопасность и её технологии.

Как и в других сферах, основными принципами сотрудничества в сфере цифровизации и информационно-коммуникационных технологий были обозначены соблюдение национальных

интересов, равенство интересов, свобода действий и ответственность, прозрачность.

10 ноября 2020 года в Москве главы государств-участников ШОС выступили с заявлением по сотрудничеству в области обеспечения международной информационной безопасности. В нем была отмечена озабоченность использованием информационно-коммуникационных технологий в целях, несовместимых с задачами поддержания международного и регионального мира, безопасности и стабильности.

Кроме того, подтверждалась общность подходов к обеспечению международной информационной безопасности. Подчеркивалось также, что разработка и использование информационно-коммуникационных технологий, а также международное и региональное сотрудничество в данной сфере, должны основываться на общепризнанных принципах международного права, включая Устав ООН.

Вместе с тем государства-участники ШОС подтверждают необходимость достижения баланса между безопасностью и развитием, что требует совместных усилий всех стран в целях обеспечения равной, справедливой и недискриминационной среды для ведения бизнеса в области новых технологий, а также разработки в рамках международных специализированных учреждений общепризнанных технических стандартов для обеспечения информационной безопасности.

Развивая сотрудничество в данном направлении, в 2021 году в Душанбе был подписан План взаимодействия стран ШОС по вопросам обеспечения международной информационной безопасности на 2022-2023 гг., разработанный при активном участии Узбекистана.

Сочетая в себе комплексный и всеобъемлющий подходы, План взаимодействия предполагает:

- изучение и обмен опытом по действующим нормативным правовым актам в сфере международной информационной безопасности, в частности, в области защиты критической информационной инфраструктуры;
- обмен сведениями, в том числе технического характера, о компьютерных инцидентах с целью своевременного обнаружения, предотвращения и ликвидации последствий компьютерных атак;
- взаимодействие в правоохранительной сфере по расследованию преступлений, связанных с использованием ИКТ, в том числе в террористических целях;
- проведение консультаций в рамках Группы экспертов ШОС по международной информационной безопасности (*действует с 2006 года*) в целях выработки единых подходов к проведению экспертиз, исследований и оценок в области обеспечения информационной безопасности;
- повышение квалификации кадров и проведение совместных учений в сфере информационной безопасности.

Анализируя нормативно-правовую и институциональную базу взаимодействия стран-участниц ШОС в рамках обеспечения информационной безопасности, следует обратить внимание на следующие моменты.

Во-первых, государства ШОС выступают за совершенствование механизмов и мер по предотвращению межгосударственных конфликтов, преодолению дефицита доверия между государствами, который может возникать вследствие противоправного использования информационно-коммуникационных технологий.

При этом межгосударственное взаимодействие основывается на принципах Устава ООН, включая уважение государственного суверенитета, политической независимости, территориальной целостности, суверенное равенство государств, урегулирование споров мирными способами, невмешательство во внутренние дела других государств, а также уважение основных свобод и

прав человека.

Во-вторых, принимая во внимание трансграничную природу киберугроз, страны ШОС признают важность международного сотрудничества в области обеспечения информационной безопасности путем активизации усилий на национальном, двустороннем и многостороннем уровнях.

В то же время продвигаемые международные инициативы в данной сфере опираются на сбалансированный и всеобъемлющий подход, учитывают национальный опыт и специфику развития государств, и, самое главное, – реализуются путем консенсуса.

В-третьих, разрабатываемые программы сотрудничества направлены в первую очередь на преодоление цифрового разрыва, повышение информационной безопасности, обеспечение равного и безопасного доступа к современным информационно-коммуникационным технологиям.

Объединяя усилия, страны ШОС получают синергетический эффект от совместного использования инфраструктуры и ресурсов, коллективного ответа на современные вызовы и угрозы в киберпространстве.

В целом, деятельность ШОС подтверждает намерения государств скоординировано принимать меры для реагирования на угрозы безопасности в информационной сфере. На сегодняшний день выработка единых подходов и мер позволяет минимизировать риски и не допустить использования информационно-коммуникационных технологий в противоправных целях.

С учетом злободневности данной темы на сегодняшний день, предстоящий Саммит ШОС в Самарканде создаст площадку для принятия скоординированных и взаимодополняющих решений в области информационной безопасности, укрепления стратегического консенсуса и сотрудничества в сфере безопасности. Это значительно повысит результативность работы, проводимой государствами на пространстве организации.

Тимур Ахмедов,

Руководитель отдела Института стратегических и межрегиональных исследований при Президенте
Республики Узбекистан