Эксперт ИСМИ: Обеспечение кибербезопасности – важный фактор устойчивого развития пространства ШОС

Повестка государств-членов ШОС по осуществлению комплексных мер в области технологической и цифровой трансформации в последние годы приобретает особую стратегическую значимость. Нельзя не отметить, что этому способствовала и пандемия коронавируса, резко повысившая спрос на ИКТ. Спровоцированные ею глобальные кризисные явления явно обозначили необходимость ускорения автоматизации производства, в т.ч. с использованием технологий искусственного интеллекта, цифровизации общественно-значимых услуг, бизнес-процессов и логистики, углубления научно-технического партнерства и активизации интернет-торговли.

В этой связи Президент Узбекистана, выступая на сегодняшнем саммите глав государств ШОС, не случайно акцентировал внимание на необходимости создания на пространстве организации совместной площадки по борьбе с киберпреступностью. Практическая значимость указанной инициативы подтверждается не только складывающейся нестабильной обстановкой в современную цифровую эпоху,
но и растущим инновационным потенциалом ШОС. Располагая совокупной экономикой в четверть мирового ВВП, 15% мирового экспорта и человеческим потенциалом почти в половину населения мира, эта организация имеет все возможности для становления в качестве глобальной цифровой платформы, облегчающей многосторонние контакты между странами-партнерами.

Вместе с тем наращивание технологической и информационной инфраструктуры, как во всем мире, так и на пространстве ШОС, определяет необходимость обеспечения ее эффективной и обновляемой защиты. Сфера кибербезопасности постоянно меняется, но очевидно, что киберугрозы становятся все более серьезными и происходят все чаще, учитывая растущее слияние ключевых отраслей экономики и в целом общественных коммуникаций с онлайн-технологиями. За последние 12 месяцев число пользователей Интернета в мире увеличилось на **3,7 %,** достигнув **5,03** млрд. к июлю т.г. При этом из них порядка **2** млрд. составляет население стран ШОС.

Кроме того, по экспертным оценкам, **85%** нарушений в сфере кибербезопасности в мире вызваны человеческим фактором, а около **71**% злоумышленных действий в киберпространстве совершаются в целях извлечения прибыли. При этом глобальные затраты на решение последствий киберпреступлений будут расти на **15**% в год в течение следующих пяти лет, достигнув **10,5** трлн долларов ежегодно к 2025-му (по сравнению с 3 трлн. долларов в 2015 году).

Особое беспокойство, помимо кибератак на социально-экономическую и финансовую инфраструктуру, представляют попытки использования ИКТ для масштабирования преступной деятельности по запугиванию и преследованию граждан, распространению дезинформации, вовлечению их в противоправную деятельность, вербовке в экстремистские организации.

Таким образом, киберпреступность сегодня являет серьезную угрозу не только для частного сектора и отдельных лиц, но и для правительств и наций в целом. Не могут не вызывать озабоченность риски применения кибератак стран для достижения односторонних конкурентных преимуществ в политической и экономической плоскостях.

В данном контексте объединение усилий на пространстве ШОС по противодействию современным киберугрозам и вызовам, принятие мер по укреплению защищенности своего информационного и киберпростанства станет качественным воплощением предложения инициативы главы Узбекистана. Это особенно важно, учитывая актуальную повестку ШОС по расширению состава организации, что несомненно повлечёт и значительное увеличение инновационного и технологического потенциала организации.

Азиз Енгалычев

Главный научный сотрудник ИСМИ при Президенте Республики Узбекистан