Проект

Резолюция

об усовершенствовании правового поля в сфере кибербезопасности в регионе ОБСЕ

Учитывая интенсивное развитие информационных технологий в мире, внедрение автоматизированных автономных систем управления в многочисленных отраслях, а также сферах стратегического значения, массовое распространение коммуникационных систем, увеличение объемов торговых, финансовых оборотов в электронном формате, всемирные тенденции накапливания и использования информации, в том числе и персональных данных,

Парламентская Ассамблея ОБСЕ

1.Выступает за усовершенствование и соответствие правового поля в государствах участниках Организации по безопасности и сотрудничеству Европы,

2.Отмечает важность сотрудничества по обеспечению и усовершенствованию правовых норм /киберзаконов/ в сверах управления производственными механизмами, обслуживающими и бытовыми электронными приборами и роботами, транспортными, в том числе судоходными и авиационными, средствами,

3.Призывает разработать общую законодательную базу по безопасности в киберпространстве, обеспечивающую защиту от ряда рисков при **использовании данных предоставляемых космическими спутниками, при пользовании социальными сетями, электронной почтой, в том числе государственной и дипломатической перепиской, и отдельными коммуникационными порталами и чатами,**

4.Заявляет о необходимости принятия мер по обеспечению защитных киберзаконов относящихся **к здравоохранительной сфере, к области управления оборонными системами и**

касающихся автоматизированных и программируемых избирательных процессов,

5.Считает важным неотлагательно обеспечить взаимодействие стран ОБСЕ и международных структур по усилению **правового контроля за электронными финансовыми операциями, оборотами электронной торговли, интернет зонами азартных игр.**

Признавая тенденцию увеличения масштабов нарушений и преступлений в киберпространстве, Парламентская Ассамблея ОБСЕ выражает озабоченность в связи с этим и отмечает существующие следующие риски:

1.Вымогательство путем использования незаконного доступа к компьютерам, мобильным устройствам, аккаунтам в социальных сетях и кабинетам в общедоступных сайтах и т.д.

2.Хулиганство, распространение материалов незаконного характера, подстрекательство, пропаганда насилия, терроризма и призывы к насильственным действиям,

3.Распространение наркотических средств, формул синтетических наркотиков /спайсов/ и другой информации по изготовлению различных наркотиков,

4. Мошенничество, обманные операции с движимым и недвижимым имуществом, драгоценными металлами и камнями, антиквариатом и т.д.

5.Финансовые пирамиды, “отмывание“ денежных средств, незаконные азартные игры, ложные лотереи, подставные или нереальные брокерские махинации, продажа несуществующих на реальном рынке ценных бумаг и т.д.

6.Фальшивые аукционы, несуществующие в реальной жизни интернет магазины, ложные благотворительные акции,

7.Преследование, незаконный сбор персональных данных и их использование, идентификация лиц,

8.Незаконное прослушивание голосовых переговоров или отслеживание и просмотр переписок, а также фото и видеоматериалов.

9. Предложение незаконных или нереальных услуг мошеннического характера,

10.Международная, военная, промышленная, деловая, политическая шпионская деятельность,

11.Распространение вирусов /вредоносных программ/ с целью вредительства, либо в рамках одного или нескольких вышеперечисленных пунктов,

Поскольку при реализации почти всех перечисленных преступлений или незаконных действий злоумышленники в общей цепи событий частично или полностью действуют в интернет пространстве, то нередко их действия выпадают за рамки уголовного права регулирующего ответственность за преступления в реальной жизни по причине отсутствия законов относящихся к конкретным действиям в интернете или с использованием интернета.

С учетом существования отдельных законов относящихся к противодействию преступлений в киберпространстве в ряде стран ОБСЕ, а также соответствующей конвенции Совета Европы, соглашения Организации Объединенных Наций, договора стран НАТО, и поправок к указанным документам, Парламентская Ассамблея ОБСЕ признает необходимость детализации киберзаконов относительно существующих рисков и имеющих место преступлений. Необходимы своевременная разработка и принятие таких законодательных актов, существование которых регулировало бы преступления совершаемые путем интернета или при частичном использовании глобальной сети.

Подчеркивая существенную роль Организации по Безопасности и Сотрудничеству Европы по воздействию на своевременное принятие законодательства в регионе ОБСЕ в соответствии с требованиями современного демократического общества и правового общественного сознания мирового сообщества, Парламентская Ассамблея ОБСЕ настоятельно рекомендует парламентам государств участников ОБСЕ разработать “киберкодекс” (подробное законодательство по кибернетической безопасности).