Секция «Международное право»

Международно-правовые проблемы обеспечения информационной безопасности в связи с использованием глобальной сети «Интернет»

Научный руководитель – Малиновский Олег Николаевич

Лихачев Никита Александрович
Студент (специалист)
Кубанский государственный университет, Краснодар, Россия
E-mail: mr.lihachev.nikita@mail.ru

10 февраля 2007 г. можно рассматривать как поворотную дату в современных международных отношениях. В этот день на Мюнхенской конференции по безопасности выступил Президент Российской Федерации В.В. Путин. Позже по значимости выступления его будут сравнивать с У. Черчиллем, с его знаменитой Фултонской речью 5 марта 1946 года. В своем выступлении В.В. Путин затронул очень важный аспект международной безопасности - безопасность информационную.

5 декабря 2016 г. Указом Президента РФ №646 была утверждена «Доктрина информационной безопасности Российской Федерации», в п. 19, в котором констатируется: «Отсутствие международно-правовых норм, регулирующих межгосударственные отношения в информационном пространстве, а также механизмов и процедур их применения, учитывающих специфику информационных технологий, затрудняет формирование системы международной информационной безопасности, направленной на достижение стратегической стабильности и равноправного стратегического партнерства» [1].

На сегодняшний день в силу определенных разногласий государствам не удалось выработать единую международно-правовую базу и общую концепцию обеспечения информационной безопасности и сформировать эффективный механизм защиты прав и свобод человека и гражданина в этой области и, в частности, в глобальной сети «Интернет», посредством которой передается и распространяется огромный объем информации. Современный мир сегодня уже невозможно представить без интернета. Однако наряду с безусловными позитивными свойствами интернет несет в себе и угрозы. При этом отметим, что заключенная в рамках Совета Европы в 2001 г. Конвенция о киберпреступности по территориальной сфере действия и по кругу регулируемых вопросов объективно не может претендовать на решение всех проблем в рассматриваемой сфере.

Постоянными пользователями сети во всем мире являются как дети, так и взрослые. Очевидно, что несовершеннолетние во многих случаях не готовы к восприятию такого потока информации и не в состоянии самостоятельно оценить ее «вредность» или «полезность». Через социальные сети их психологически обрабатывают, доводят до самоубийств, распространяют информацию наркотической и порнографической направленности. В интернете растет число «фейковых» сайтов, ведется работа по вербовке террористов и экстремистов. В какой-то степени — это можно назвать новым методом экстремистской и террористической деятельности, так как её цель - дестабилизация социальной обстановки, подрыв авторитета государства как системы, которая должна обеспечивать безопасность граждан, и, конечно же, формирование в массовом сознании мнения о том, что правоохранительные органы бессильны перед новыми опасностями.

Цель любого противостояния - локального конфликта или крупной войны - вложить как можно меньше средств для достижения победы над противником. Поэтому в современных условиях глобализации на первый план выходит информационное воздействие. Гораздо эффективнее, не применяя традиционное оружие, обрушить банковскую систему государства, взломать базы данных секретной информации, вывести из строя объекты жизнеобеспечения, в том числе устроить аварии на особо опасных объектах, таких как ГЭС или АЭС, что может нанести колоссальный ущерб государству и привести к огромным жертвам и как следствие экономического и политическому кризису. Таким образом, можно сделать вывод, что ведение боевых действий между государствами может быть менее эффективным, чем применение вредоносных информационных технологий, которые становятся все более востребованными.

Исходя из того, что проблемы обеспечения информационной безопасности на универсальном, региональном, межрегиональном и национальных уровнях взаимосвязаны, необходим комплексный подход к их решению. Представляется, что решению указанных проблем могли бы способствовать следующие меры:

1) на универсальном уровне – консолидация усилий государств, стоящих на позициях создания единого международного информационного правопорядка, по принятию Кодекса информационной безопасности, относящегося к актам международного«мягкого права», и Конвенции ООН об обеспечении международной информационной безопасности [2]. Отметим, что Россия, выступающая за обеспечение примата международного права в регулировании международных отношений, является одним из инициаторов принятия Кодекса и разработчицей проекта указанной Конвенции;

2) на региональном и межрегиональном уровнях: максимальное задействование потенциала СНГ, ОДКБ и ШОС. С учетом нынешних политических реалий представляется, что сотрудничество России в рамках этих организаций по рассматриваемым проблемам на данном этапе может быть наиболее эффективным. Государства-члены указанных организаций могли бы выработать и закрепить на договорном уровне понятия «информационная безопасность»применительно к сети «Интернет», «информационное оружие», «информационный терроризм», «информационные угрозы»; создать центры обеспечения информационной безопасности и противодействия киберпреступности.

Так как ОДКБ является военизированной организацией, то одной из её приоритетных задач является защита военных объектов от хакерских атак, защита военных секретов и документации под грифом «совершенно секретно». Механизм обеспечения коллективной информационной безопасности ОДКБ можно было бы закрепить путем внесения дополнений в уже принятую Стратегию коллективной безопасности ОДКБ до 2025 года [3].

Страны, входящие в данные организации, могли бы начать структуризацию интернета. Создание единого реестра сайтов на национальных уровнях позволило бы более эффективно отслеживать и пресекать действия различных преступных элементов, реализуемые через сайты суицидной, экстремисткой, террористической, наркотической, порнографической направленности. Ужесточение правового положения социальных сетей также способствовало бы противодействию терроризма и других негативных явлений.

Осуществление указанных мер в рамках СНГ, ОДКБ и ШОС может вывести данные организации на продвинутый уровень в регулировании проблем обеспечения информационной безопасности, являющейся важнейшим компонентом всеобъемлющей системы международной безопасности, и дать импульс их решению на универсальном уровне.

Анализируя структурное состояние интернета можно прийти к выводу, что данные огромного количества пользователей - граждан государств-членов СНГ совершенно незащищены, так как большинство доменных имен и IP-адресов контролируется международной организацией ICANN, созданной в 1998 г. при участии правительства США [4], то есть информация, обрабатываемая через эти домены, идет через ICANN. Поэтому формирование собственной системы маршрутно-адресной информации в рамках СНГ позволит обеспечить сохранность информации пользователей сети «Интернет». Целесообразно в рамках СНГ сформировать комиссию, целью которой будет контроль над инфраструктурой сети «Интернет». На государственном уровне уже сегодня необходимо создавать систему контроля информационных потоков для того, чтобы исключить существование «безликих», «фейковых» пользователей, проникающих в российский сегмент интернета, в том числе из-за рубежа, в целях совершения преступлений террористической и экстремисткой направленности.

Источники и литература

1) Доктрина информационной безопасности Российской Федерации от 6 декабря 2016 г.// https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.
2) Конвенция об обеспечении международной информационной безопасности (концепция) // URL: http://www.scrf.gov.ru.
3) Стратегия коллективной безопасности Организации Договора о коллективной безопасности на период до 2025 года //URL: http://www.odkb-csto.org/documents/detail. php?ELEMENT_ID=8382.
4) Сайт международной коммерческой компании ICANN //URL: https://www.icann.org/ru