Секция «Обеспечение финансовой безопасности России: финансовые расследования в цифровой экономике»

Проблема применимости международного права к институту информационной безопасности

Научный руководитель – Хабибулин Алик Галимзянович

Советов Денис Игоревич
Сотрудник
Московский государственный университет имени М.В.Ломоносова, Высшая школа государственного аудита, Кафедра экономических и финансовых расследований, Москва, Россия
E-mail: sovetov-work@mail.ru

Влияние информационно-коммуникационных технологий (ИКТ) на все аспекты жизни человека, общества и государства трудно переоценить. Наряду с очевидными благами с точки зрения экономического, социального и культурного развития повышение роли ИКТ в современном мире неизбежно влечет новые риски для международной и национальной безопасности.

Мир уже получил реальные свидетельства тому, что ущерб от применения ИКТ в целях, противоречащих Уставу ООН, а также в криминальных и террористических целях может быть сопоставим с наиболее разрушительными видами оружия. В список потенциальных «мишеней» для атак с использованием информационного оружия попадают не только информационные ресурсы сети Интернет, но и объекты критически важной инфраструктуры государств в сфере промышленности, транспорта, энергетики. При этом масштаб и технологический уровень подобного деструктивного воздействия неуклонно возрастают.

Россия традиционно рассматривает проблему обеспечения МИБ через призму единой «триады»:

- угроз военно-политического;
- террористического;
- криминального характера.

Ежегодно мировая экономика теряет сотни миллиардов долларов от использования ИКТ в криминальных целях. Реальностью стало повсеместное использование террористическими группировками достижений в сфере ИКТ. И все же в последнее время внимание мирового сообщества сосредоточено в большей степени на военно-политическом компоненте «триады». Все чаще государства, обладающие более совершенными ИКТ, стремятся использовать это преимущество для упрочения своего положения на международной арене, что неминуемо ведет к конфронтации, новым угрозам международной безопасности, нарушению стабильности и конфликтам. Более масштабной становится милитаризация информационного пространства, все легче становится «нажать на спусковой крючок», начав боевые действия с «невидимой и безмолвной» войны с использованием ИКТ.

Основная проблема заключается в том, что в настоящее время отсутствует на высоком уровне Конвенция «об обеспечении международной информационной безопасности». Россия придерживается позиции о необходимости формирования подобного акта.

В рамках внутренней системы права России, возможно выделить следующие ключевые акты, направленные на обеспечение информационной безопасности: №149-ФЗ «Об информационной безопасности» — данный акт устанавливает основные права и обязанности, касающиеся информации и информационной безопасности; № 152-ФЗ «О персональных

данных» — данный закон описывает правила работы с персональными данными различных категорий; №98-ФЗ «О коммерческой тайне» — в рамках обозначенного документа определяются: понятие, особенности и порядок хранения коммерческой тайны компаний; №68-ФЗ «Об электронной подписи» — дает определение электронной подписи и описывает, особенности ее применения и уровень юридической силой свойственной подобному информационному ресурсу; №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» - описывает правила защиты IT-инфраструктуры на предприятиях, работающих в сферах, критически важных для государства. К таким сферам относится здравоохранение, наука, оборона, связь, транспорт, энергетика, банки и некоторая промышленность.

Таким образом возможно определить, что внутренняя система источников права, регулирующих информационные правоотношения в России представляют собой относительно проработанную структуру. Однако, в международном праве возможно обнаружить ряд проблем, что вызывает ряд сложных международно-правовых вопросов:

· Применимо ли международное право к киберпространству?

· Какие действия возможно считать угрозой информационной безопасности государства и суверенитету?

· Возникает ли у государства право на самооборону в случае возникновения информационной угрозы?

Каждый из данных вопрос представляется необходимым раскрыть в рамках международного сотрудничества при формировании Конвенции об обеспечении информационной безопасности на высоком уровне.

Источники и литература

1) Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» // СПС Консультант Плюс
2) Федеральный закон «О коммерческой тайне» от 29.07.2004 N 98-ФЗ // СПС Консультант Плюс
3) Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ // СПС Консультант Плюс
4) Федеральный закон «Об электронной подписи» от 06.04.2011 № 63-ФЗ // СПС Консультант Плюс
5) Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ // СПС Консультант Плюс
6) Применимость международного права к киберпространству: иллюзия или реальность? / В.Н. Трофимов. – М.: Юстицформ, 2021. -182 с.