Секция «Национальная внешняя политика в меняющейся международной среде»

Киберпреступность как новый вызов национальной безопасности РФ: проблемы и пути их решения

Научный руководитель – Рамазанова Пати Казихановна

Салихова Патимат Ражабдибировна
Студент (бакалавр)
Российская правовая академия МЮ РФ, Северо-Кавказский филиал, Юридический факультет, Кафедра гуманитарных и социально — экономических дисциплин, Махачкала, Россия
E-mail: salikhova.patimat1999@mail.ru

Проблема создания надёжной системы национальной безопасности в современном мире относится к числу перспективных задач развития государства и его законодательства. Практически все государства сегодня сталкиваются со специфическими угрозами национальной безопасности. В основном, эти угрозы обусловлены стремительно и динамично развивающимися технологиями. Речь идёт о набирающем обороты с каждым днём теневом интернете, неконтролируемых фискальной системой расчетах, мгновенном неправомерном обмене информацией. Все эти процессы создали идеальную среду для киберпреступности. Многие сферы человеческой деятельности сегодня также переместились в виртуальное пространство: общение, обучение, банковские операции, покупки и хранение информации.

Жертвами преступлений, совершаемых в виртуальной среде становятся и российские граждане. Более того, по данным международной службы по обеспечению безопасности в киберпространстве Symantec Security [1] список стран с высоким уровнем совершаемых преступлений в виртуальной среде возглавляет именно Россия. Вследствие этого преступления в виртуальном пространстве, или киберпреступления, становятся особой сферой внимания экспертов в области национальной безопасности нашего государства. Так, Центробанк РФ в декабре 2016 года заявил об ущербе в размере 2 млрд. руб, которые похитили со счетов российских банков. Резонансной стала история столичного Металлоинвестбанка, со счетов которого хакеры украли более 200 млн. руб. Денежные средства были украдены путем несанкционированного доступа к терминалам управления корреспондентских счетов учреждений ЦБ, начали несанкционированно отправлять с него деньги на сторонние счета частных лиц.

Отсутствие эффективных механизмов борьбы с киберпреступлениями определяется сегодня как одна из угроз национальной безопасности нашего государства. Более того, ни одно государство сегодня не способно противостоять этому злу самостоятельно. Очевидна потребность в активизации международного сотрудничества, для которого является актуальным, в частности, налаживание международно-правового механизма регуляции. Однако существуют нюансы.

Во-первых, данная работа замедляется из-за процессов на международной арене: столкновение интересов различных государств, отсутствие взаимопонимания и сложность достижения консенсуса в геополитических интересах по сути способствуют развитию и распространению киберпреступности. Между тем, обмен опытом в данной сфере представляет собой стратегический интерес. В мире есть примеры достаточно эффективных систем противодействия совершению киберпреступлений. В настоящее время ведущие страны мира активно расширяют и создают в вооруженных силах и спецслужбах подразделения, которые должны обеспечивать развитие наступательных возможностей в киберпространстве. Например, в США наряду с уже функционирующим Центром национальной

кибербезопасности в составе Вооруженных сил сформировано Объединенное кибернетическое командование, которое в глобальном масштабе должно координировать усилия всех структур Пентагона в ходе ведения боевых действий, оказывать соответствующую поддержку гражданским федеральным учреждениям, а также взаимодействовать с аналогичными по задачам ведомствами других стран [2]

Во-вторых, нередко при международном регулировании борьбы с киберпреступностью, возникают проблемы из-за отличий национальных стандартов в сфере кибербезопасности; отсутствии четкого унифицированного категориального аппарата; недостаточном уровне координации деятельности правоохранительных органов при расследовании киберпреступлений, низком уровне обмена информацией о киберинцидентах между государствами; недостаточном уровне государственно-частного сотрудничества[3] Позиция Российской Федерации заключается в необходимости разработки под эгидой ООН новой Конвенции по противодействию преступлений в сфере использования информационно-коммуникационных технологий, которая как по содержанию, так и по географии своего применения, должна носить универсальный характер, учитывать реалии всех без исключения государств.

Проведенный анализ позволяет сделать вывод о важности роли законодательства в сфере обеспечения национальной безопасности. Она связана с созданием условий для полноценного функционирования государства и необходимой разработкой новой парадигмы безопасности России с учетом современного понимания ее государственных интересов и системы стратегических приоритетов. Необходимо найти фундаментальные решения в области обеспечения национальной безопасности для достижения оптимального соотношения между национальными интересами страны и приоритетными направлениями ее развития. Таким образом, для совершенствования национальной безопасности Российской Федерации необходимо предпринять следующие действия:

Во-первых, важным шагом для обеспечения информационной безопасности РФ может стать инициатива по созданию международной нормативно-правовой базы, регулирующей отношения в киберпространстве. К примеру международной конвенции, о киберпступности под эгидой ООН. Такая инициатива уже поступала, однако мы предлагаем отобразить в данном акте киберпреступност не в целом как глобальную проблему, но и учитывать особенности их проявления в каждом отдельном государстве.

Во-вторых, мы считаем, что необходимо создать центры по борьбе с киберпреступностью на уровне регионов, со странами которых РФ осуществляет наиболее широкое взаимодействие. К примеру СНГ, АТР. Их создание может стать более продуктивным способом противодействия, так как будет сформирован из сотрудников правоохранительных органов государств-участников вышеназванных организаций. Они будут действовать на основании международного договора, пользоваться экстерриториальностью и подчиняться напрямую Совету министров внутренних дел государств - участников Содружества Независимых Государств, а также в АТР.

В-третьих, считаем целесообразным рассмотреть опыт зарубежных стран, в частности США в борьбе с киберпреступностью, проанализировать перспективы создания аналогичных органов в вооружённых силах РФ.

Источники и литература

1) Бутусова Л.И. К вопросу о киберпреступности в международном праве. // Вестник экономической безопасности. М., 2016. No. 2. С. 37

2) Нарутто С.В., Е.М. Якимова Международное сотрудничество в борьбе с киберпреступностью. М., 2016. С. 3

3) Симантик.ру: https://www.symantec.com/ru/ru