Жебриков Василий Витальевич, 3 курс, РАНХиГС при Президенте РФ.

Роль Вьетнама в выстраивании системы безопасности в региональном (АСЕАН) информационно-коммуникационном пространстве в рамках диалога с ЕАЭС и Российской Федерацией.

Обеспечение информационной безопасности в текущий момент обозрения, вне всяких сомнений, ввиду многомерности и многоаспектности явления, взаимозависимости и взаимообусловленности отраслей научно-практического приложения, синхронизации процессов глобального общественного развития, как вид деятельности являет собой поистине трансграничный феномен, выраженный во взаимопроникновении разнонаправленных явлений реального, физического мира посредством порождённых(генерируемых) кибернетическим пространством виртуальных операций, выраженных, в общем смысле, в направленности на противодействие угрозам сверхнового и нон-конвенционального характера, связанных активными неправомерными, противоправными цифровыми актами, имеющими в качестве объекта посягательства социальный порядок, суверенитет, политическую независимость, государственные интересы, международный мир и безопасность.

Именно поэтому, в условиях диверсификации и расширения значения и роли фактора цифровизации как международного значимого явления, разработка автономной, самостоятельной, отвечающей требованиям и специфике политико-экономического содержания геополитической макрорегиональной политики в процессе конструирования архитектуры кибербезопасности стала магистральной и, во многом, лидирующей повесткой, которая, невзирая на национально-ориентированные внешнеполитические тенденции и иные противоречия, смогла объединить интересы всех государств-членов АСЕАН.

В контексте всего вышеприведённого особая роль отводится ***Вьетнаму***, благодаря инициативе и активному участию которого были достигнуты многие поставленные цели и задачи, являющиеся ключевыми факторами взаимного сближения и кооперации стран-членов АСЕАН в вопросах коллективной кибербезопасности.

В первую очередь, необходимо заострить внимание на том, что ***Вьетнам***, имея особое и, во многом, даже важное, если не ключевое для региона ***Юго-Восточной Азии***, геополитическое положение(членство в ***АСЕАН***, выход к ***Южно-Китайскому морю***, территориальная близость к ***Китаю***, относительно сопредельное нахождение к Австралии как одному из государств-членов военно-морского альянса ***AUKUS*** и англо-саксонского разведывательного сообщества ***Five Eyes***) всегда находится под пристальным и усердным

вниманием стран ***«Коллективного Запада»***, в особенности ***США***, имеющих свои собственные активно претворяемые в жизнь внешнеполитические интересы в контексте глобального пространства ***Азиатско-Тихоокеанского Региона***, обусловленные, в первую очередь, официальными и декларируемыми публично пунктами ***Стратегии национальной безопасности 2022 года***, маркирующими в пределах конфронтации с ***КНР Индийско-Тихоокеанский регион***(в вопросе влияния в ***Южно-Китайском море***) как важнейшее и магистральное измерение геостратегической конкуренции[1].

Как обозначено выше, постоянное внимание ***США к Вьетнаму*** не остаётся исключительно в разрабатываемых перспективных долгосрочных положениях государственной доктрины общемирового однополярного господства, а, непосредственно, выражается в систематических и постоянных неправомерных актах, выраженных в осуществлении информационно-технологического воздействия в виртуально-кибернетическом пространстве посредством компьютерно-электронных средств на критическую цифровую инфраструктуру ***Вьетнама***, обуславливающую её суверенитет и политическую независимость. Так, по информации вьетнамского ***Центра реагирования на компьютерные угрозы (ЦРКУ)***, за весь 2017 год было зафиксировано свыше 40 тыс. кибератак с совокупным ущербом более 400 млн долл. (особо показателен тот факт, что только в ***Агрибанке*** киберпреступники взломали более 400 личных счетов), а в, свою очередь, по данным специализирующейся на обеспечении информационной и сетевой безопасности вьетнамской компании ***BKAV***, число случаев взлома и заражения вирусами локальных сетей и персональных компьютеров во ***Вьетнаме*** ежегодно увеличивается примерно на 10%(так, в октябре 2014 года была проведена целенаправленная атака на крупнейшего хостинг-провайдера ***Vietnam Communications***, когда несколько сайтов, размещенных на площадках компании, были выведены из строя). В 2019 году, по данным ***«Лаборатории Касперского»***, вьетнамские пользователи сталкиваются более чем с 800 тыс. атак со стороны вредоносного кода, и около 21,5% интернет-пользователей Вьетнама подвержены риску стать жертвами кибератаки. Как позже подтвердил ***Эдвард Сноуден***, международные неправительственные организации, благотворительные фонды и различные юридические лица, получающие финансирование и консультации из-за рубежа при поддержке диппредставительств, будучи частью нелегальной резидентуры внешней

[1] Стратегия национальной безопасности США. [Электронный ресурс].–Режим доступа: https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf

разведки ***ЦРУ***, целенаправленно подготавливали и организовывали данные хакерские атаки против ***Вьетнама***[2].

В связи со всем вышесказанным, ***Вьетнам***, оказавшись одним из первоочерёдных объектов посягательств в виртуально-компьютерной сфере со стороны американских спецслужб, предпринял на национальном уровне комплекс значимых мер, предопределивших не только исключительно его одностороннее политическое развитие, но и, в существенной степени, обозначивших контуры региональных(***АСЕАН***) и межгосударственных и межправительственных инициатив. Речь, безусловно, идёт о нашумевшем ***Законе «О сетевой информационной безопасности»(состоит из 7 глав и 43 статей)***, вступившим в силу в 2019 году и ставшим одним из самых флагманских актов национального внутреннего права своего времени, который на уровне своего исчерпывающего единого нормативного юридически обязывающего содержания закреплял в числе передовых направлений кибербезопасности следующие положения:

1)Обеспечение безопасности информационно-коммуникационных технологий является обязательством не только компетентных контрольно-надзорных государственных структур, но и различных организаций и даже независимых частных лиц, что, в свою очередь, предполагало наделение юридических и физических лиц отдельными публично-властными функциями или, говоря более точно, публично-властными обязательствами;

2)Обработка сетевых инцидентов, инспекционные мероприятия, развёртывание сети в целях охраны национальной цифровой инфраструктуры, связанной с алгоритмами интернет-маршрутизации, и международного шлюза реализуется с соблюдением законных прав и интересов организаций и отдельных лиц, режима государственной тайны, в связи с чем предусмотрена процедура предоставления сведений IT-компаниями и операторами локальных сетей с иностранным компонентом уполномоченным должностных правительственным лицам на регулярной, законодательно установленной основе.

3) Противоправные деяния, совершаемые в форме специальных виртуально-цифровых операций и посягающие на конкретный сегмент общественных отношений, в зависимости от юридических значимых признаков квалифицируются в соответствии с конкретными элементами составов преступлений в виде кибершпионажа, сетевого терроризма и экстремизма, отрицания фактов национальной истории, подрыва национального единства(

[2] С.Довгий, В.Колотов, Н.Сторожук. Влияние кибербезопасности на суверенитет страны и перспективы российско-вьетнамского сотрудничества// Первая Миля. 6/2019. С. 42-48.

статьи 17, 18, 19, 20, 21), что позволяет однозначно определять объект уголовно-правовой охраны[3].

Впоследствии многие уникальные решения, отражённые в национальном правотворчестве Вьетнама и других заявлениях политического характера, нашли, при непосредственном всестороннем участии Ханоя, своё прямое отражение в актуальной деятельности ***АСЕАН*** как региональной организации интеграции в рамках тех межгосударственных многосторонних форматов кооперации и содействия, которые связаны со стратегическим участием ***ЕАЭС или Российской Федерации***. Так, в свою очередь, в ноябре 2018 года, когда Закон «О сетевой информационной безопасности» ***Вьетнама*** уже был одобрен ***Национальной Ассамблей*** и подписан, при активном участии ***Ханоя*** состоялся ***третий саммит Российская Федерация-АСЕАН***, по результатам которого было принято ***Совместное заявление о стратегическом партнёрстве***, в упомянутом в ***Совместном заявлении о стратегическом партнёрстве*** были обозначены конкретные направления деятельности в указанной сфере:

1) Активизация совместных усилий по сокращению цифрового разрыва;

2) Наращивание национальных потенциалов и запуск образовательных программ и тренингов по различным вопросам безопасности в сфере использования информационно-коммуникационных технологий;

3) Укрепление практического сотрудничества по безопасности в сфере использования информационно-коммуникационных технологий на таких направлениях, как борьба с использованием ИКТ в террористических целях и для иной преступной деятельности;

4) Содействие укреплению и оптимизации существующих региональных механизмов по безопасности в сфере использования информационно-коммуникационных технологий;

5) Рассмотрение ***АСЕАН*** инициативы ***Российской Федерации*** об учреждении ***Диалога Россия - АСЕАН*** по вопросам, относящимся к безопасности ИКТ[4].

В тоже самое время был подписан ***Меморандум о взаимопонимании между ЕЭК и АСЕАН*** в области экономического сотрудничества, где в качестве одного из векторов многостороннего взаимодействия фиксировался процесс всеобъемлющей цифровой

---

[3]Закон «О кибербезопасности» Вьетнама (принят на 12.06.2018 г. на 5-й сессии Национального Собрания Вьетнама). [Электронный ресурс]. –Режим доступа: https://letranlaw.com/insights/vietnam-cybersecurity-law-2022-legal-regulations/#What_is_the_Cybersecurity_Law_of_2018

[4] Совместное заявление 3-го саммита Российская Федерация-АСЕАН о стратегическом партнёрстве, 14 ноября 2018 года. [Электронный ресурс]. –Режим доступа: http://kremlin.ru/supplement/5360

трансформации, в том числе в аспектах обеспечения безопасности, управления данными и снижения рисков.

Помимо всего прочего, благодаря отчётливо выраженной позиции ***Ханоя***, всегда акцентирующего внимания на острой теме обеспечения национальной безопасности и недопущения экстремистских явлений в сетевом пространстве посредством посягательства на внутренние дела и критическую инфраструктуру в контексте ***Стратегии сотрудничества АСЕАН в области кибербезопасности на 2021-2025 годы*** отдельным столпом стоят пункты о создании механизма и разработке консолидированного, долгосрочного плана сотрудничества в сфере образовательной деятельности внутри интеграционного объединения при поддержке стран-партнеров по диалогу (особо выделяются государства-члены ***ЕАЭС в качестве важнейших партнёров***) в целях создания устойчивого киберпространства в ***АСЕАН***[5].

Подходя к завершению, можно однозначно утверждать, что Вьетнам, будучи одним из главных участников становления цифровизации в области обеспечения безопасности на субрегиональном(АСЕАН) уровне и осознавая свою ответственность за продвижение актуальных предложений, демонстрирует пример разнонаправленных, многоуровневых передовых, флагманских инициатив, которые становятся воплощённой реальностью в контексте вектора межгосударственных и универсальных многосторонних отношений в области коллективной кибербезопасности.

[5]Стратегии сотрудничества АСЕАН в области кибербезопасности на 2021-2025 годы. [Электронный ресурс]. –Режим доступа: http://kremlin.ru/supplement/5360 https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf

Список литературы:

1)Закон «О кибербезопасности» Вьетнама (принят на 12.06.2018 г. на 5-й сессии Национального Собрания Вьетнама). [Электронный ресурс]. –Режим доступа: https://letranlaw.com/insights/vietnam-cybersecurity-law-2022-legal-regulations/#What_is_the_Cybersecurity_Law_of_2018

2) Стратегия национальной безопасности США. [Электронный ресурс].–Режим доступа: https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf

3) С.Довгий, В.Колотов, Н.Сторожук. Влияние кибербезопасности на суверенитет страны и перспективы российско-вьетнамского сотрудничества// Первая Миля. 6/2019. С. 42-48.

4) Совместное заявление 3-го саммита Российская Федерация-АСЕАН о стратегическом партнёрстве, 14 ноября 2018 года. [Электронный ресурс]. –Режим доступа: http://kremlin.ru/supplement/5360

5) Стратегии сотрудничества АСЕАН в области кибербезопасности на 2021-2025 годы. [Электронный ресурс]. –Режим доступа: http://kremlin.ru/supplement/5360 https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf