Секция «Внешняя политика США и ЕС»

Обеспечение кибербезопасности в рамках многостороннего сотрудничества (на примере НАТО, ЕС)

Научный руководитель – Вершинина Ирина Михайловна

Толстов Дмитрий Викторович
Студент (магистр)
Московский государственный университет имени М.В.Ломоносова, Факультет глобальных процессов, Направление глобальной экономики и управления, Москва, Россия
E-mail: ya.nde201276@gmail.com

Современный мир стал свидетелем бурного развития информационных технологий, которые безусловно делают нашу жизнь проще и комфортнее. Однако, за новыми технологиями приходят новые угрозы, связанные с кибербезопасностью.

НАТО и ЕС признают необходимость защиты от кибератак. У каждой из этих организаций есть свои программы по кибербезопасности. Необходимо рассмотреть стратегии кибербезопасности на примере НАТО, ЕС используемые этими организациями в борьбе за защищенность своих информационных ресурсов.

НАТО

Кибербезопасность имеет центральное значение в политике НАТО. Она рассматривается как один из ключевых элементов коллективной защиты. В рамках своей стратегии, НАТО проводит широкомасштабные учения для подготовки своих членов к действию в случае кибератаки. Кроме того, НАТО активно сотрудничает со своими партнерами по всему миру, чтобы обеспечивать безопасность на международном уровне.

В настоящее время, НАТО считает, что кибератаки являются одним из главных вызовов для международной безопасности. Поэтому, организация продолжает улучшать свою киберзащиту и исследует новые методы борьбы с киберугрозами.

Европейский Союз

Европейский союз также придает большое значение кибербезопасности, рассматривая ее как один из приоритетов международной политики. ЕС имеет свою стратегию кибербезопасности, которая регулярно обновляется в соответствии с изменяющимися требованиями.

Одной из главных задач ЕС является защита критической информационной инфраструктуры. Для этого, ЕС инвестирует в развитие технологий, направленных на обнаружение и борьбу с киберугрозами. Также, ЕС активно сотрудничает со своими членами, чтобы разработать общие критерии кибербезопасности, которые будут приниматься всеми странами ЕС.

Обеспечение кибербезопасности в рамках многостороннего сотрудничества на примере Европейского союза.

В свете все чаще возникающих случаев кибератак и киберпреступлений, кибербезопасность становится все более приоритетным вопросом для европейских стран. Европейский союз (ЕС) признает важность обеспечения кибербезопасности и активно работает в этом направлении.

Для обеспечения кибербезопасности в рамках многостороннего сотрудничества ЕС создал несколько инструментов и механизмов. Например, ЕС создал Европейское агентство по кибербезопасности (ENISA) с целью обеспечения координации, сотрудничества и совместной работы в области кибербезопасности между европейскими государствами.

Европейский союз также запустил программу по укреплению кибербезопасности в рамках европейской инфраструктуры, которая включает в себя стандартизацию и сертификацию кибербезопасности для критически важных инфраструктур, таких как банки, телекоммуникации и энергетика.

В дополнение к этому, ЕС сотрудничает с другими международными организациями и государствами в области кибербезопасности. Например, ЕС и НАТО заключили соглашение о сотрудничестве в области кибербезопасности, а также ЕС подписал соглашения с США, Россией, Канадой и другими странами для обмена информацией и сотрудничества в борьбе с киберпреступностью.

ЕС также признает необходимость обучения и подготовки кадров в области кибербезопасности. ЕС инвестирует средства в исследования и обучение в области кибербезопасности, а также проводит курсы и тренинги для специалистов из различных областей, чтобы повысить их компетенцию в области кибербезопасности.

Таким образом, ЕС активно работает в области обеспечения кибербезопасности, используя многостороннее сотрудничество и координацию между государствами и международными организациями. Однако, в свете все более сложных и интенсивных кибератак, ЕС должен продолжать улучшать свои механизмы обеспечения кибербезопасности и сотрудничать с другими странами для более эффективной и сильной защиты от киберугроз.

Источники и литература

1) Резолюция, принятая Генеральной Ассамблеей 27 декабря 2013, 68/243. Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности. [Электронный ресурс] URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N13/454/05/PDF/N1345405.pdf?OpenElement (дата обращения: 22.02.2024).
2) The Common Security and Defence Policy. [Электронный ресурс] URL: https://www.eeas.europa.eu/eeas/common-security-and-defence-policy_en (дата обращения: 22.02.2024).
3) The North Atlantic Treaty Organization. [Электронный ресурс] URL: http://www.nato.int/nato-welcome/index.html (дата обращения: 22.02.2024).
4) Action against Cybercrime. Council of Europe. [Электронный ресурс] URL: https://www.coe.int/en/web/cybercrime (дата обращения: 22.02.2024).
5) NATO-EU: a strategic partnership. [Электронный ресурс] URL: https://www.fransamaltingvongeusau.com/documents/dl2/h6/2.6.17.pdf (дата обращения: 22.02.2024).
6) EU-NATO Declaration on ESDP. [Электронный ресурс] URL: https://www.nato.int/cps/en/natolive/official_texts_19544.htm (дата обращения: 22.02.2024).