Секция «Международная безопасность: новые вызовы и угрозы»

Политика Китая и России в сфере информационной безопасности.

Научный руководитель – Кумпан Вадим Александрович

Пешков Станислав Алексеевич
Студент (бакалавр)
Кубанский государственный университет, Факультет истории, социологии и международных отношений, Краснодар, Россия
E-mail: mulinelli4444@list.ru

Интернет стал главным проводником и хранилищем информации. С одной стороны это облегчило обмен информацией, улучшило возможности реагирования на те или иные события, однако это и стало новой потенциальной угрозой. Появились возможности перехвата огромных объёмов информации начиная личной информацией пользователей заканчивая секретами государственной важности. Для сохранения данной информации и для контроля за её потоками государства должны осуществлять новую политику, принимать новые решения. В 21 веке военные действия могут вестись теперь, не только на суше, на море или в воздухе , но и в киберпространстве. На нашей планете формируется новое бесконечная цифровая сеть, охватывающая всю Землю, и люди используют её с каждым годом его все больше и больше . Режим самоизоляции в этом году, связанный с эпидемией коронавируса, дополнительно стимулировал приток людей в интернет пространство. Стратегическая задача любой страны в 21 веке - это защита своего киберпространства. Подходы к обеспечению такой защиты у каждой страны индивидуальные.

В данной работе рассмотрены стратегии России и Китая в сфере информационной безопасности. На данный момент, Россия и Китай занимают лидирующие позиции в сфере разработок и информационной безопасности.

Многие рейтинговые агентства ставят Россию в первую пятерку государств#_ftn1. Как и многие страны, стремящиеся обеспечить свою кибербезопасность, Российская Федерация имеет свою нормативно-правовую базу, однако данные документы не имеют системного характера и требуют логического структурирования.#_ftn2 Что касается финансирования то Россия поступательно увеличивает финансирование проектов связанных с информационной безопасностью. Только на один проект «Информационная безопасность» направленный на создание безопасной и устойчивой информационной инфраструктуры для граждан, представителей бизнеса и государства в цифровом пространстве будет потрачено 16 миллиардов рублей в 2022 и 2023 годах.#_ftn3 Наращивание финансирования в данной отрасли оправдано её стратегическим значением. По части технического оснащения Россия отстает от конкурентов. Существует зависимость информационной безопасности РФ от иностранных поставщиков программно-аппаратных компонентов программного обеспечения (ПО) и оборудования. Так, большинство интернет-технологий (браузеры, поисковики, социальные сети, операционные системы) находится вне пределов российского контроля. Это создает дополнительные угрозы безопасности. Поэтому для обеспечения своего суверенитета государству следует иметь полную технологическую цепочку, начиная от процессора и заканчивая конечным ПО.#_ftn4

Китай обладает второй по силе кибермией в мире а по финансированию уступает лишь США согласно исследованию Zecurion.#_ftn5 Самыми знаменитым китайским проектом в области информационной безопасности является «Золотой щит». В нормативно-правовом аспекте обеспечения информационной безопасности необходимо отметить , что у КНР ведет активную деятельность в этой области с 1997 года , и на середину 2020 года обладает полной нормативно-правовой базой так и национальной стратегией. В 2017

году в КНР был принят законе о кибербезопасности, который предусматривает, что все госучреждения и ключевые инфраструктурные операторы должны использовать «безопасные и контролируемые» технологии. Предусмотрено, что в 2020 году государственные организации и учреждения заменят 30% зарубежного «железа» и «софта» на китайские. В 2021 году этот процент составит 50%, и оставшиеся 20% будут заменены в 2022 году.#_ftn6

Подводя итоги, можно сказать, что Китай обладает нормативно правовой базой и национальной стратегией, тогда как Россия находится на пути формирования своей доктрины. Обе страны выделяют все больше денег на проекты в сфере информационной безопасности. Также обе страны имеют зависимость от иностранных поставщиков программно-аппаратных компонентов программного обеспечения и оборудования. Стоить отметить, что защита информации в Интернете и её регулирование это новые задачи, с которыми человечество ранее не сталкивалось. Если Китай является одним из лидеров в проектах по цифровизации общества, Россия делает первые шаги на этом пути, и может получить нужный опыт от китайских партнёров.

Источники и литература

1) 1)В интернет ввели кибервойска https://www.kommersant.ru/doc/3187320
2) 2) Д.А. Литвинов Оценка политики России в сфере кибербезопасности https://cyberleninka.ru/article/n/otsenka-politiki-rossii-v-oblasti-kiberbezopasnosti-i-vozmozhnye-varianty-ee-sovershenstvovaniya/viewer Дата обращения :24.10.2020
3) 3)«Без финансирования невозможно»: как Россия поборется с киберпреступностью https://www.gazeta.ru/tech/2020/10/15_a_13319947.shtml Дата обращения :24.10.2020
4) 4)Н.Ромашкина Информационный суверенитет или почему России нужна стратегия информационной безопасности https://russiancouncil.ru/analytics-and-comments/analytics/informatsionnyy-suverenitet-ili-pochemu-rossii-nuzhna-strategiya-informatsionnoy-bezopasnosti/ Дата обращения :24.10.2020
5) 5) Аналитики Zecurion составили первый в мире рейтинг кибервойск https://www.zecurion.ru/press/7538/ Дата обращения :24.10.2020
6) 6) «Цифровой» Китай: Опора на собственные силы https://svpressa.ru/economy/article/278766/ Дата обращения :24.10.2020