Impact Factor: 9.2 ISSN-L: 2544-980X

УГРОЗА ИНФОРМАЦИОННЫХ ВОЙН НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ.

Шарипова У. Б. Асс., Юлдашев О.И.[1]

Аннотации*: В современном информационном обществе информационные войны представляют серьезную угрозу для национальной безопасности. Возрастающая связность и зависимость от информационных технологий создают новые возможности для атак и манипуляций в сфере информации. В данной статье мы рассмотрим угрозы информационных войн и меры, которые можно предпринять для защиты национальной безопасности.*
Ключевые слова: *борьбы, Дезинформация, манипуляции, Шпионаж и киберразведка*

Кибератаки: Кибератаки являются одним из наиболее опасных аспектов информационных войн. Хакеры и киберпреступники могут направлять атаки на национальные информационные системы, компьютерные сети и критическую инфраструктуру. Это может привести к краже конфиденциальных данных, нарушению функционирования государственных учреждений и даже возможности причинения физического ущерба. Для борьбы с этой угрозой необходимо улучшение киберзащиты, регулярное обновление программного обеспечения, обучение персонала и сотрудничество с международными партнерами.

Дезинформация и манипуляции: Информационные войны также включают распространение дезинформации и манипуляции с целью влиять на общественное мнение и государственные процессы. Злоумышленники могут использовать социальные сети, псевдонимы и поддельные аккаунты для распространения ложной информации, дестабилизации общества и нарушения доверия к государственным институтам. Противодействие этой угрозе включает образование общества, критическое мышление, развитие медиа-грамотности и разработку алгоритмов обнаружения и фильтрации дезинформации.

Шпионаж и киберразведка: Информационные войны также связаны с шпионажем и киберразведкой. Государства и киберпреступные группировки могут использовать средства кибератак для сбора разведывательной информации о национальной безопасности, экономике и политической ситуации. Противодействие этой угрозе требует разработки и применения сильных криптографических алгоритмов, усиления защиты сетей и сотрудничества с разведывательными организациями.

Уязвимости промышленной инфраструктуры: Критическая промышленная инфраструктура, такая как электроэнергетика, транспорт и коммуникации, становится объектом интереса в информационных войнах. Атаки на эти системы могут вызвать серьезные последствия, включая прекращение работы, нарушение услуг и даже угрозу жизни людей. Для

[1] Самаркандский филиал Ташкентского университета, информационных технологий имени Мухаммада ал-Хорезми

обеспечения безопасности промышленной инфраструктуры необходимо внедрение защитных мер, мониторинг состояния систем и разработка планов реагирования на чрезвычайные ситуации.

Заключение: Угрозы информационных войн национальной безопасности являются серьезным вызовом в нашей цифровой эпохе. Необходимо разработать и реализовать комплексные стратегии по киберзащите, образованию общества и сотрудничеству между государствами для эффективного противодействия этим угрозам. Только через совместные усилия и инновационные подходы мы сможем защитить национальную безопасность и обеспечить устойчивость информационного пространства.

Литературы:

1. https://www.kaspersky.ru/resource-center/definitions/what-is-cloud-security

2. https://www.eset.com/ua-ru/about/newsroom/blog/business-security/khraneniye-dannykh-kompaniy-v-oblachnom-khranilishche-naskolko-eto-seychas-bezopasno-ru.