MINISTRY OF EDUCATION OF THE REPUBLIC OF BELARUS
BELARUSIAN STATE UNIVERSITY
FACULTY OF INTERNATIONAL RELATIONS
Department of International Law

Annotation to the master's thesis

INTERNATIONAL LEGAL FRAMEWORK FOR CYBERSECURITY

Cui Kaidi

Scientific supervisor –
PhD, Associate Professor
Maroz Nataliya

Minsk, 2025

ANNOTATION

1.Structure and scope of the master's thesis : 58 p, 58 sources.

2.Key words: CYBERSECURITY, INTERNATIONAL LAW, STATE SOVEREIGNTY, REGIONAL COOPERATION, CYBER TERRORISM, CRITICAL INFRASTRUCTURE, INSTITUTIONAL MECHANISMS

3.The purpose of this work is to analyze international legal regulation of cybersecurity, its challenges, and future prospects.

4.The object of the work is international legal relations on cybersecurity, including in regional context.

5.Research methods are theoretical overview analysis, synthesis, legal comparison, historical comparison.

6.Research Results and Novelty: the research results highlight the multi-faceted nature of cybersecurity, integrating technical, legal, and geopolitical dimensions. It identifies key international legal frameworks (e.g., UN GGE reports, SCO agreements) and regional practices (EU's NIS 2, African Union convention), analyzing their effectiveness and gaps. The work confirms that cybersecurity threats require a hybrid governance model combining hard law (existing international treaties) and soft law (voluntary norms), with regional mechanisms, where practical efforts are undertaken (like SCO's cyber counter-terrorism exercises and China-ASEAN cooperation serving as practical cases).

Novelty lies in its emphasis on balancing cyber sovereignty with global collaboration, proposing a "progressive legislation" approach to address technological evolution. It critiques the fragmentation of current norms and advocates for inclusive governance, highlighting developing countries' roles (e.g., African Union's capacity building). The study also innovatively links emerging technologies (AI, quantum computing) to legal frameworks, urging proactive governance models to prevent regulatory lag.

АННОТАЦИЯ

1.Структура и объем дипломной работы: Страница 58, 58 источника.

2.Ключевые слова: Кибербезопасность, международное право, государственный суверенитет, региональное сотрудничество, кибертерроризм, критическая инфраструктура, институциональные механизмы

3.Целью данной работы является анализ международного правового регулирования кибербезопасности, его проблем и перспектив развития.

4.Объектом работы международные отношения по поводу международно-правового регулирования кибербезопасности, в том числе, в региональном контексте.

5.Методы исследования: анализ и синтез, сравнительно-правовой метод, исторический метод.

6.Результаты и новизна исследования: Результаты исследования подчеркивают многогранный характер кибербезопасности, рассматривая технические, правовые и геополитические измерения проблемы. В нем анализируются ключевые международные правовые основы (например, доклады ГГЭ ООН, соглашения ШОС) и региональная практика (Директива ЕС о кибербезопасности, Конвенция Африканского союза о кибербезопасности и защите персональных данных), анализируется их эффективность и пробелы. Работа подтверждает, что угрозы кибербезопасности требуют гибридной модели управления, сочетающей твердое право (существующие международные договоры) и мягкое право (нормы, предполагающие их добровольное соблюдение), с региональными механизмами, где осуществляются такие практические мероприятия как киберконтртеррористические учения ШОС; двустороннее сотрудничество (например, между Китаем и АСЕАН, служащими в качестве практических примеров).

Новизна заключается в том, что исследование делает акцент на балансировании киберсуверенитета с глобальным сотрудничеством, предлагая «прогрессивное законодательство» для решения проблемы технологической эволюции. В работе критикуется фрагментация существующих норм. Автор выступает за инклюзивное управление, подчеркивая роль развивающихся стран (например, наращивание потенциала Африканского союза). Автор также указывает на необходимость регулировать применение новых технологий (ИИ, квантовые вычисления) нормами международного парва, призывая к проактивным моделям управления для предотвращения задержек в регулировании.