



«ПЕРСПЕКТИВЫ СТРАТЕГИЧЕСКОГО СОТРУДНИЧЕСТВА
РОССИЙСКОЙ ФЕДЕРАЦИИ И КИТАЙСКОЙ НАРОДНОЙ
РЕСПУБЛИКИ
В РАМКАХ ОРГАНИЗАЦИОННО–ПРАВОВОГО ОБЕСПЕЧЕНИЯ
МЕЖДУНАРОДНОЙ И НАЦИОНАЛЬНОЙ ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ»

ЗВЕРЯНСКАЯ ЛАРИСА ПАВЛОВНА –
ИНСТИТУТ ГОСУДАРСТВА И ПРАВА
РОССИЙСКОЙ АКАДЕМИИ НАУК



Отсчет активного развития российско–китайского сотрудничества в области МИБ можно начать с момента подписания Председателем КНР Цзян Цзэмином и Президентом РФ В. В. Путиным в июле 2001 г. Договора о добрососедстве, дружбе и сотрудничестве, в котором на законодательном уровне закрепилось состояние «добрососедских, партнерских и дружеских отношений».



Российско-китайские отношения характеризуются высокой динамикой развития, прочной правовой базой, разветвленной организационной структурой и активными связями на всех уровнях.

Современные российско-китайские отношения официально определяются сторонами как всеобъемлющее равноправное доверительное партнерство и стратегическое взаимодействие.

ОСОБЕННОСТИ ОРГАНИЗАЦИОННО–ПРАВОВОГО ОБЕСПЕЧЕНИЯ МЕЖДУНАРОДНОЙ И НАЦИОНАЛЬНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ КИТАЙСКОЙ НАРОДНОЙ РЕСПУБЛИКИ

- Закон КНР «О государственной безопасности» от 01.07.2015;
- Закон КНР «О кибербезопасности» от 07.11.2016;
- «Стратегия международного сотрудничества КНР в киберпространстве» опубликованная 1 марта 2017.

ЗАКОН КНР «О ГОСУДАРСТВЕННОЙ БЕЗОПАСНОСТИ» ОТ 01.07.2015

Положениями закона, закрепляется то, что государство создает системы обеспечения сетевой и информационной безопасности, улучшает возможности для охраны сетевой и информационной безопасности, использования сетевых и информационных технологий, обеспечивает безопасность и подконтрольность основных сетевых и информационных технологий, ключевых объектов инфраструктуры, важнейших информационных систем и данных, укрепляет регулирование сетей, предупреждает, пресекает и в соответствии с законодательством наказывает за сетевые атаки, вторжение в сети, кражи в сетях, распространение незаконной и вредной информации и другие противоправные и преступные деяния в сетях, защищает суверенитет, безопасность, развитие государством сетевого пространства.

ЗАКОН КНР «О КИБЕРБЕЗОПАСНОСТИ» ОТ 07.11.2016

- «Сетевая безопасность» определяется как способность предотвращать сетевые атаки, вторжения, повреждения, несанкционированный доступ и использование, непредвидимые происшествия, посредством осуществления необходимых мер для поддержания устойчивой и надежной работы сети, обеспечения целостности, конфиденциальности и удобства использования сетевых данных.
- Под «критически важной информационной инфраструктурой» понимается область государственных коммуникационных и информационных услуг, энергетики, дорожного и иного транспорта, ирригации, финансов, государственных услуг, электронного правительства и других ключевых отраслей и секторов, а также другая иная информационная инфраструктура, нанесение ущерба, незаконное использование и утечка данных и которой могут нести серьезную угрозу национальной безопасности, национальному благополучию, жизни людей и общественным интересам.

«СТРАТЕГИЯ МЕЖДУНАРОДНОГО СОТРУДНИЧЕСТВА КНР В КИБЕРПРОСТРАНСТВЕ» ОПУБЛИКОВАННАЯ 1 МАРТА 2017.

В Стратегии содержится призыв к упорному отстаиванию суверенного равенства (интернет–суверенитета), отказу от гегемонии в Интернете, а также невмешательству во внутренние дела других государств.

Китай выделяет в качестве основных проблем и угроз киберпространства несбалансированность развития, несправедливый порядок, расширение «цифровой пропасти» между странами и регионами, уязвимость критической информационной инфраструктуры.

Особое внимание обращается на угрозу кибертерроризма, развитие информационной преступности, а также вмешательство государств во внутренние дела других стран путем злоупотребления ИКТ, массового кибершпионажа.

В качестве стратегических целей КНР, при участии в международном сотрудничестве в киберпространстве, определены:

- 1. Защита интернет–суверенитета, национальной безопасности и интересов Китая;
- 2. Формирование системы международных правил в киберпространстве;
- 3. Содействие справедливости в управлении Интернетом;
- 4. Защита законных прав и интересов граждан;
- 5. Содействие глобальному сотрудничеству в цифровой экономике;
- 6. Создание платформ для культурного обмена.

ОСНОВНЫЕ ТЕНДЕНЦИИ И ПЕРСПЕКТИВЫ СТРАТЕГИЧЕСКОГО СОТРУДНИЧЕСТВА РФ И КНР:

- Достижение и подписание соглашений по сотрудничеству в области обеспечения международной информационной безопасности;
- Взаимодействие в разработке и продвижении норм международного права в целях обеспечения национальной и международной информационной безопасности;
- Обмен информацией о законодательстве государств по вопросам обеспечения информационной безопасности;
- Содействие совершенствованию международно-правовой базы и практических механизмов сотрудничества в обеспечении международной информационной безопасности;
- Углубление сотрудничества и координации деятельности государств по проблемам обеспечения международной информационной безопасности в рамках международных организаций и форумов;
- Содействие научным исследованиям в области обеспечения международной информационной безопасности, проведение совместных научно-исследовательских работ, совместная подготовка специалистов, обмен студентами, аспирантами и преподавателями профильных высших учебных заведений;
- Создание каналов связи и контактов в целях совместной разработки и продвижении стратегических соглашений в сфере МИБ (например, сотрудничество Лиги безопасного Интернета и Общества информационно безопасности Китая).
- В рамках сотрудничества по кибербезопасности началась разработка системы интернет-контроля Red Web для российского сегмента сети Интернет.

The image features a dark blue gradient background with white circuit board traces and nodes in the corners. The traces are thin lines that branch out and connect to small circles, resembling a network or data flow diagram. The text is centered in a white, italicized serif font.

БЛАГОДАРЮ ЗА ВНИМАНИЕ.