

Л.Н.Гумилев атындағы
Еуразия ұлттық
университеті
Халықаралық қатынастар
факультеті
Аймақтану кафедрасы



Евразийский
национальный университет
им. Л.Н.Гумилева
Факультет международных
отношений
Кафедра регионоведения

«Отандастар қоры»
коммерциялық емес
акционерлік қоғамы



Некоммерческое акционерное
общество
«Отандастар қоры»

«АЙМАҚТАНУДЫҢ ҚАЗІРГІ КЕЗЕҢДЕГІ МӘСЕЛЕЛЕРІ»
ХАЛЫҚАРАЛЫҚ ҒЫЛЫМИ-ПРАКТИКАЛЫҚ КОНФЕРЕНЦИЯ
МАТЕРИАЛДАРЫНЫҢ ЖИНАҒЫ

«СОВРЕМЕННЫЕ ПРОБЛЕМЫ РЕГИОНОВЕДЕНИЯ»
СБОРНИК МАТЕРИАЛОВ МЕЖДУНАРОДНОЙ НАУЧНО-
ПРАКТИЧЕСКОЙ КОНФЕРЕНЦИИ



**Л. Н. Гумилев атындағы Еуразия ұлттық университеті
Халықаралық қатынастар факультеті
Аймақтану кафедрасы**

«Отандастар қоры» коммерциялық емес акционерлік қоғамы

**Евразийский национальный университет им. Л.Н. Гумилева
Факультет международных отношений
Кафедра регионоведения**

Некоммерческое акционерное общество “Фонд Отандастар”

«АЙМАҚТАНУДЫҢ ҚАЗІРГІ МӘСЕЛЕЛЕРІ»

**ХАЛЫҚАРАЛЫҚ ҒЫЛЫМИ-ПРАКТИКАЛЫҚ КОНФЕРЕНЦИЯ
МАТЕРИАЛДАРЫНЫҢ ЖИНАҒЫ**

**СБОРНИК МАТЕРИАЛОВ МЕЖДУНАРОДНОЙ НАУЧНО-ПРАКТИЧЕСКОЙ
КОНФЕРЕНЦИИ**

«СОВРЕМЕННЫЕ ПРОБЛЕМЫ РЕГИОНОВЕДЕНИЯ»

27 наурыз 2023, Астана

УДК 327
ББК 66.4
А31

А31 «Аймақтанудың қазіргі мәселелері» халықаралық ғылыми-практикалық конференция = Международная научно-практическая конференция «Современные проблемы регионоведения». – Астана: – 247 б. - қазақша, орысша, ағылшынша.

ISBN 978-601-337-861-1

Жинаққа ғалымдардың, докторанттардың, магистранттар мен студенттердің аймақтық даму мен аймақты зерттеуге әсер ететін проблемаларды түсінуге жәрдемдесуге бағытталған баяндамалар кірді. Бұл процестерді әр түрлі аспектілерде және әр түрлі жағынан қарастыру әсіресе қазіргі кезде өзекті болып табылады.

В сборник вошли доклады ученых, докторантов, магистрантов и студентов, направленные на содействие более глубокому пониманию проблем, влияющих на региональное развитие и изучение региона. Рассмотрение данных процессов в разных аспектах, и с разных сторон особенно актуально в наши дни.

УДК 327
ББК 66.4

ISBN 978-601-337-861-1

©Л.Н. Гумилев атындағы
Еуразия ұлттық университеті, 2023

2. Юрлов Ф.Н. Китай, Индия, США: баланс изменений силы // Азия и Африка сегодня. – 2013. – №1. – С.2-9.
3. Campbell I. India's role in Central Asia. – London: Safeworld, 2013. – 14 p.
4. Kavalski E. India and Central Asia: the Mythmaking and International Relations of Rising Power. – London; New York: Taurus, 2010. – 288 p.
5. Make in India. URL: <https://www.makeinindia.com/> (дата обращения: 23.12.2017).

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СТРАНАХ ЦЕНТРАЛЬНОЙ АЗИИ

Д.Н.Аубакирова
Евразийский национальный университет им. Л.Н.Гумилева
Астана, Казахстан
a_d_n_94@mail.ru

***Аннотация.** Законодательство в сфере информационной безопасности является сравнительно молодой отраслью законодательства не только в Центральной Азии, но и в мире. Стремительное развитие информационных технологий привело к необходимости урегулирования, в том числе и правовой политики в отношении информационной безопасности. В странах Центральной Азии информационная безопасность рассматривается как одна из составляющих национальной безопасности государства. В данной работе рассматриваются основные нормативно-правовые акты в сфере информационной безопасности.*

***Ключевые слова:** информационная безопасность, кибербезопасность, Центральная Азия, информация, национальная безопасность, концепция.*

В условиях глобальных угроз обеспечение безопасности в мире требует координации и урегулирования многих политических и экономических вопросов. В частности, это продовольственные угрозы, негативные последствия изменения климата, загрязнение окружающей среды, истощение природных ресурсов и замедление их повторного возобновления, необходимость обеспечения экономного режима энергоносителями, развития «зеленой» экономики. Однако среди всех компонентов особого внимания заслуживает новый, и одновременно сложный, элемент - кибербезопасность. Кибербезопасность быстро превратилась из технической дисциплины в стратегическую концепцию.

В последние годы, особенно в период пандемии COVID-19, уровень цифровизации увеличился в несколько раз. Логично, что с ростом использования цифровых инструментов растет и объем создаваемых данных. Интернетизация все глубже и активнее трансформирует наш мир, затрагивая межличностное общение, товарные цепочки и логистический поток,

информационный обмен и в целом буквально все аспекты жизни. Влияние всемирной сети как на отдельных потребителей, так и на крупные экономики, становится все более заметным и повсеместным. Пандемия также ярко показала, как тесно взаимосвязаны все предприятия между собой и как рост цифровизации вывел население планеты на новый уровень киберугроз и атак.

Сегодня весь мир сталкивается с киберпреступностью, финансовым мошенничеством, компьютерными атаками. По данным Всемирного экономического форума, в 2018 году ущерб мировой экономике от киберпреступности составил 1,5 трлн долларов, в 2022-м прогнозируются потери в восемь трлн, а в 2030-м они могут достигнуть 90 трлн.[1] Это еще раз подтверждает тот факт, что совершенствование информационной и кибербезопасности - актуальная проблема современности.

Страны Центральной Азии все чаще подвергается повседневным проявлениям киберпреступности. Кибератаки растут пропорционально развитию цифровой инфраструктуры. В подобных условиях кибербезопасность начинает занимать первостепенную роль. Страны Центральной Азии стали уделять данному аспекту важное значение на государственном уровне.

С целью решения задач по обеспечению информационной безопасности в июне 2017 года Правительством была утверждена Концепция кибербезопасности «Киберщит Казахстана». Концепция основана на оценке текущей ситуации в сфере информатизации государственных органов, автоматизации государственных услуг, перспектив развития «цифровой» экономики и технологической модернизации производственных процессов в промышленности, расширения сферы оказания информационно-коммуникационных услуг. Документ определил основные направления реализации государственной политики в сфере защиты электронных информационных ресурсов, информационных систем и сетей телекоммуникаций, обеспечения безопасного использования информационно-коммуникационных технологий.

Помимо этого, созданы испытательные лаборатории в сфере информационной безопасности по исследованию вредоносного кода, запущен национальный координационный центр информационной безопасности, частная служба реагирования на компьютерные инциденты (CERT), 7 оперативных центров информационной безопасности (SOC), увеличено число грантов по этой специальности.[2]

Для дальнейшего улучшения ситуации в сфере информационной безопасности и защите персональных данных, Министерством цифрового развития, инноваций и аэрокосмической промышленности РК инициирован вопрос о наделении Комитета по информационной безопасности функциями по защите персональных данных, проведения аудита и проверок владельцев информационных систем, в которых обрабатываются персональные данные. Результаты работы Концепции кибербезопасности «Киберщит Казахстана» будут подведены в 2023 г., после чего планируется введение новой концепции.

В Узбекистане этому аспекту также придается важное значение на государственном уровне. Так, в Стратегии развития Нового Узбекистана на 2022-2026 годы в цели 89 определено создание системы предупреждения киберпреступности.

Вопросу усиления кибербезопасности глава государства также уделил особое внимание на совещании 14 апреля 2022-го, на котором рассмотрены достигнутые результаты в сфере информационных технологий и поставлены задачи на текущий год. Сделан акцент на критическое изучение информационных систем минис-терств и ведомств с принятием необходимых мер.[3]

Кроме того, 15 апреля этого года Президент Узбекистана подписал Закон «О кибербезопасности», состоящий из восьми глав и 40 статей. Согласно документу, защита интересов личности, общества и государства от внешних и внутренних угроз в киберпространстве - приоритет в обеспечении кибербезопасности государства. Единую государственную политику в этой области определяет лидер республики, а Служба государственной безопасности является уполномоченным государственным органом в этом направлении. Таким образом, госорганы и организации имеют право получать информацию о кибер-атаках, уязвимостях в программном обеспечении, оборудовании и технологиях от уполномоченного государственного органа в целях обеспечения кибербезопасности.

3 мая 2019 года была утверждена Концепция информационной безопасности Кыргызской Республики на 2019-2023 годы, направленная на совершенствование методов обеспечения информационной безопасности, оценку угроз информационной безопасности и создание эффективной системы противодействия в информационной сфере. В этой концепции говорится, что информационная безопасность является одной из составляющих национальной безопасности. Также подчеркивается, что защита национальных интересов, жизненных устоев и системы ценностей страны в информационной среде является важной необходимостью для обеспечения устойчивого развития и защиты личности, общества и государства.

В концепции перечислены основные проблемы информационной безопасности республики: распространение киберпреступности; незащищенность сознания граждан от опасного контента; возможность манипуляции мнением; угроза подмены государственной идеологии, вербовки; сложность контроля интернет-ресурсов; слабо развитый отечественный контент; нехватка высококвалифицированных кадров. [4]

9 декабря 2022 года президент Кыргызстана Садыр Жапаров и президент России Владимир Путин сделали совместное заявление о сотрудничестве в области международной информационной безопасности. В заявлении отмечается, что современные информационно-коммуникационные технологии все чаще используются в целях, несовместимых с целями поддержания международного мира, безопасности и стабильности, и поэтому незаконное применение этих технологий все чаще представляет угрозу для граждан,

общества и государства.[5]

На самом деле, этот документ был подписан 25 февраля 2021 года в Москве, Россия, и ратифицирован Жогорку Кенешем в ноябре того же года. Согласно пункту 6 статьи 1 документа, в списке основных угроз международной информационной безопасности значится «распространение информации, наносящей ущерб общественно-политической и социально-экономическим системам государств-участников, их духовно-нравственной и культурной среде». Это показывает, что стороны придают большое значение вопросу информационной безопасности.

В Таджикистане в настоящее время насчитывается более трех миллионов пользователей интернета, из которых свыше 80% вольно или невольно получают доступ к материалам экстремистского характера. В основном, это молодое поколение Таджикистана, которое в большинстве случаев подвержено радикальным и экстремистским идеям.

В этой связи, вопросы обеспечения информационной безопасности находится в центре внимания Правительства Республики Таджикистан. Данный вопрос в стране регулируется Концепцией информационной безопасности Республики Таджикистан от 7 ноября 2003 года. В этой концепции нашли своё отражение конкретные цели, задачи, принципы и важнейшие направления обеспечения информационной безопасности национального государства. Согласно её содержанию, «Под информационной безопасностью Республики Таджикистан понимается состояние защищённости её национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства». Перечень видов информационных угроз нашему государству определены также в этой концепции .

С целью защиты национального «киберсуверенитета» и предотвращения вредоносных хакерских атак в 2019 году в Туркменистане был принят Закон «О кибербезопасности», который определяет порядок и специфику обеспечения безопасности информационной инфраструктуры в стратегически важных отраслях. Актуальность принятого Закона, разработанного по поручению Президента Гурбангулы Бердымухамедова, определяют процессы цифровизации, широко использующиеся в Туркменистане. В структуре агентства «Türkmenaragatnaşyk» создана Государственная служба кибербезопасности, а в структурах министерств — специальные отделы. Это, наряду с принятыми соответствующими законодательными актами, повысит эффективность мер, направленных на гарантирование информационной безопасности как государства и его структур, так и частных предпринимателей, и каждого пользователя компьютерных и мобильных устройств. Наряду с этим в некоторых учебных заведениях страны осуществляется подготовка IT-специалистов.[6]

В Центральной Азии стремительно идет процесс цифровизации – как на уровне государств, так и в жизни самих людей. Электронный документооборот, цифровизация госуслуг, интернет-покупки, электронные

кошельки – все это уже прочно вошло в урбанизированную жизнь жителей региона, и этот процесс продолжается. Все страны Центральной Азии приняли множество законодательных документов, стратегий, концепций в области цифровой и кибербезопасности и стремятся наращивать свой потенциал, понимая, что в современных реалиях риски и угрозы в этой области будут только нарастать. Борьба с киберугрозами с каждым годом приобретает все большую актуальность. В связи с этим активно принимаемые в странах Центральной Азии меры по противодействию угрозам в сфере информационных технологий способствуют эффективному обеспечению безопасности.

Литература

1. Отчет Всемирного экономического форума 2021-2022 гг. [Электронный ресурс], 2022. URL: https://www3.weforum.org/docs/WEF_Annual_Report_2021_22.pdf (дата обращения: 08.03.23).
2. Информационная безопасность [Электронный ресурс], 2022. URL: <https://www.gov.kz/memleket/entities/mdai/activities/6?lang=ru> (дата обращения: 10.03.23).
3. Трансформация «Узбектелекома», кибербезопасность и новый университет: Мирзиёев провёл совещание по IT [Электронный ресурс], 2022. URL: <https://kun.uz/ru/news/2022/04/14/transformatiya-uzbektelekoma-kiberbezopasnost-i-novyy-universitet-mirziyoyev-provyol-soveshchaniye-po-it> (дата обращения: 11.03.23).
4. Концепция информационной безопасности Кыргызской Республики на 2019-2023 годы от 3 мая 2019 года № 209. URL: <http://cbd.minjust.gov.kg/act/view/ru-ru/13652> (дата обращения: 15.03.23).
5. Совместное заявление Президента Садыра Жапарова и Президента России Владимира Путина о сотрудничестве в области обеспечения международной информационной безопасности [Электронный ресурс], 2022. URL: https://www.president.kg/ru/sobytiya/23966_sovmestnoe_zayavlenie_prezidenta_sadira_ghaparova_i_prezidenta_rossii_vladimira_putina_o_sotrudnichestve_v_oblasti_obespecheniya_meghdunarodnoy_informacionnoy_bezopasnosti (дата обращения: 16.03.23).
6. Обеспечение информационной безопасности [Электронный ресурс] // «Нейтральный Туркменистан», 2021. URL: <https://science.gov.tm/news/20211127news-2021-11-26-1/> (дата обращения: 19.03.23).

**XXI ҲАСЫРДАҒЫ ҚР МЕН АҚШ ЖОҒАРЫ ДЕНГЕЙДЕГІ
ӘРІШТЕСТІК ЖӘНЕ ҮКІМЕТАРАЛЫҚ ҚАРЫМ-ҚАТЫНАСТАРЫ**