

SCIENCE
PROBLEMS.UZ

ISSN 2181-1342

Actual problems of social and humanitarian sciences
Актуальные проблемы социальных и гуманитарных наук

Ijtimoiy-gumanitar fanlarning dolzarb muammolari

8-maxsus
son (5-jild)

2025

SCIENCEPROBLEMS.UZ

**IJTIMOIIY-GUMANITAR FANLARNING
DOLZARB MUAMMOLARI**

№ 5/8 (5) – 2025

**АКТУАЛЬНЫЕ ПРОБЛЕМЫ СОЦИАЛЬНО-
ГУМАНИТАРНЫХ НАУК**

ACTUAL PROBLEMS OF HUMANITIES AND SOCIAL SCIENCES

TOSHKENT-2025

BOSH MUHARRIR:

Isanova Feruza Tulqinovna

TAHRIR HAY'ATI:

07.00.00- TARIX FANLARI:

Yuldashev Anvar Ergashevich – tarix fanlari doktori, siyosiy fanlar nomzodi, professor;

Mavlanov Uktam Maxmasabirovich – tarix fanlari doktori, professor;

Xazratkulov Abror – tarix fanlari doktori, dotsent;

Tursunov Ravshan Normuratovich – tarix fanlari doktori;

Xolikulov Axmadjon Boymahmatovich – tarix fanlari doktori;

Gabrielyan Sofya Ivanovna – tarix fanlari doktori, dotsent;

Saidov Sarvar Atabullo o'g'li – katta ilmiy xodim, Imom Termiziy xalqaro ilmiy-tadqiqot markazi, ilmiy tadqiqotlar bo'limi.

08.00.00- IQTISODIYOT FANLARI:

Karlibayeva Raya Xojabayevna – iqtisodiyot fanlari doktori, professor;

Nasirxodjayeva Dilafruz Sabitxanovna – iqtisodiyot fanlari doktori, professor;

Ostonokulov Azamat Abdukarimovich – iqtisodiyot fanlari doktori, professor;

Arabov Nurali Uralovich – iqtisodiyot fanlari doktori, professor;

Xudoyqulov Sadirdin Karimovich – iqtisodiyot fanlari doktori, dotsent;

Azizov Sherzod O'ktamovich – iqtisodiyot fanlari doktori, dotsent;

Xojayev Azizxon Saidaloxonovich – iqtisodiyot fanlari doktori, dotsent

Xolov Aktam Xatamovich – iqtisodiyot fanlari bo'yicha falsafa doktori (PhD), dotsent;

Shadiyeva Dildora Xamidovna – iqtisodiyot fanlari bo'yicha falsafa doktori (PhD), dotsent v.b.;

Shakarov Qulmat Ashirovich – iqtisodiyot fanlari nomzodi, dotsent.

09.00.00- FALSAFA FANLARI:

Hakimov Nazar Hakimovich – falsafa fanlari doktori, professor;

Yaxshilikov Jo'raboy – falsafa fanlari doktori, professor;

G'aybullayev Otabek Muhammadiyevich – falsafa fanlari doktori, professor;

Saidova Kamola Uskanbayevna – falsafa fanlari doktori;

Hoshimxonov Mo'min – falsafa fanlari doktori, dotsent;

O'roqova Oysuluv Jamoliddinovna – falsafa fanlari doktori, dotsent;

Nosirxodjayeva Gulnora Abdukaxxarovna – falsafa fanlari nomzodi, dotsent;

Turdiyev Bexruz Sobirovich – falsafa fanlari doktori (DSc), Professor.

10.00.00- FILOLOGIYA FANLARI:

Axmedov Oybek Saporbayevich – filologiya fanlari doktori, professor;

Ko'chimov Shuxrat Norqizilovich – filologiya fanlari doktori, dotsent;

Hasanov Shavkat Ahadovich – filologiya fanlari doktori, professor;

Baxronova Dilrabo Keldiyorovna – filologiya fanlari doktori, professor;

Mirsanov G'aybullo Qulmurodovich – filologiya fanlari doktori, professor;

Salaxutdinova Musharraf Isamutdinovna – filologiya fanlari nomzodi, dotsent;

Kuchkarov Raxman Urmanovich – filologiya fanlari nomzodi, dotsent v/b;

Yunusov Mansur Abdullayevich – filologiya fanlari nomzodi;

Saidov Ulugbek Aripovich – filologiya fanlari nomzodi, dotsent.

12.00.00- YURIDIK FANLAR:

Axmedshayeva Mavlyuda Axatovna – yuridik fanlar doktori, professor;

Muxitdinova Firyuza Abdurashidovna – yuridik fanlar doktori, professor;

Esanova Zamira Normurotovna – yuridik fanlar doktori, professor, O'zbekiston Respublikasida xizmat ko'rsatgan yurist;

Hamroqulov Bahodir Mamasharifovich – yuridik fanlar doktori, professor v.b.,;

Zulfiqorov Sherzod Xurramovich – yuridik fanlar doktori, professor;

Xayitov Xushvaqt Saparbayevich – yuridik fanlar doktori, professor;

Asadov Shavkat G'aybullayevich – yuridik fanlar doktori, dotsent;

Ergashev Ikrom Abdurasulovich – yuridik fanlari doktori, professor;

Utemuratov Maxmut Ajimuratovich – yuridik fanlar nomzodi, professor;

Saydullayev Shaxzod Alixanovich – yuridik fanlar nomzodi, professor;

Hakimov Komil Baxtiyarovich – yuridik fanlar doktori, dotsent;

Yusupov Sardorbek Baxodirovich – yuridik fanlar doktori, professor;

Amirov Zafar Aktamovich – yuridik fanlar doktori (PhD);

Jo'rayev Sherzod Yuldashevich – yuridik fanlar nomzodi, dotsent;

Babadjanov Atabek Davronbekovich – yuridik fanlar nomzodi, professor;

Normatov Bekzod Akrom o'g'li — yuridik fanlar bo'yicha falsafa doktori;

Rahmatov Elyor Jumaboyevich — yuridik fanlar nomzodi;

13.00.00- PEDAGOGIKA FANLARI:

Xashimova Dildarxon Urinboyevna – pedagogika fanlari doktori, professor;

Ibragimova Gulnora Xavazmatovna – pedagogika fanlari doktori, professor;

Zakirova Feruza Maxmudovna – pedagogika fanlari doktori;

Kayumova Nasiba Ashurovna – pedagogika fanlari doktori, professor;

Taylanova Shoxida Zayniyevna – pedagogika fanlari

doktori, dotsent;

Jumaniyozova Muhayyo Tojiyevna – pedagogika fanlari doktori, dotsent;

Ibraximov Sanjar Urunbayevich – pedagogika fanlari doktori;

Javliyeva Shaxnoza Baxodirovna – pedagogika fanlari bo'yicha falsafa doktori (PhD);

Bobomurotova Latofat Elmurodovna — pedagogika fanlari bo'yicha falsafa doktori (PhD).

19.00.00- PSIXOLOGIYA FANLARI:

Karimova Vasila Mamanosirovna – psixologiya fanlari doktori, professor, Nizomiy nomidagi Toshkent davlat pedagogika universiteti;

Hayitov Oybek Eshboyevich – Jismoniy tarbiya va sport bo'yicha mutaxassislarni qayta tayyorlash va malakasini oshirish instituti, psixologiya fanlari doktori, professor

Umarova Navbahor Shokirovna– psixologiya fanlari doktori, dotsent, Nizomiy nomidagi Toshkent davlat pedagogika universiteti, Amaliy psixologiyasi kafedrasini mudiri;

Atabayeva Nargis Batirovna – psixologiya fanlari doktori, dotsent;

Shamshetova Anjim Karamaddinovna – psixologiya fanlari doktori, dotsent;

Qodirov Obid Safarovich – psixologiya fanlari doktori (PhD).

22.00.00- SOTSIOLOGIYA FANLARI:

Latipova Nodira Muxtarjanovna – sotsiologiya fanlari doktori, professor, O'zbekiston milliy universiteti kafedra mudiri;

Seitov Azamat Po'latovich – sotsiologiya fanlari doktori, professor, O'zbekiston milliy universiteti;

Sodiqova Shohida Marxaboyevna – sotsiologiya fanlari doktori, professor, O'zbekiston xalqaro islom akademiyasi.

23.00.00- SIYOSIY FANLAR

Nazarov Nasriddin Ataqulovich –siyosiy fanlar doktori, falsafa fanlari doktori, professor, Toshkent arxitektura qurilish instituti;

Bo'tayev Usmonjon Xayrullayevich –siyosiy fanlar doktori, dotsent, O'zbekiston milliy universiteti kafedra mudiri.

OAK Ro'yxati

Mazkur jurnal Vazirlar Mahkamasi huzuridagi Oliy attestatsiya komissiyasi Rayosatining 2022-yil 30-noyabrdagi 327/5-son qarori bilan tarix, iqtisodiyot, falsafa, filologiya, yuridik va pedagogika fanlari bo'yicha ilmiy darajalar yuzasidan dissertatsiyalar asosiy natijalarini chop etish tavsiya etilgan ilmiy nashrlar ro'yxatiga kiritilgan.

“Ijtimoiy-gumanitar fanlarning dolzarb muammolari” elektron jurnali 2020-yil 6-avgust kuni 1368-sonli guvohnoma bilan davlat ro'yxatiga olingan.

Muassis: “SCIENCEPROBLEMS TEAM” mas'uliyati cheklangan jamiyati

Tahririyat manzili:

100070. Toshkent shahri, Yakkasaroy tumani, Kichik Beshyog'och ko'chasi, 70/10-uy. Elektron manzil:

scienceproblems.uz@gmail.com

Bog'lanish uchun telefon:

(99) 602-09-84 (telegram).

07.00.00 – TARIX FANLARI

<i>Choriyeva Nargiza Ibotovna</i> O'ZBEKISTONDA TURIZM VA EKOTURIZMNI RIVOJLANTIRISH: SAMARQAND VILOYATINING SALOHIIYATI	8-11
--	------

08.00.00 – IQTISODIYOT FANLARI

<i>Xudayarova Zuhra, Turayev Baxtiyor</i> HUDUDDA ASALARICHILIK FAOLIYATINING UY XO'JALIKLARI DAROMADLARIGA TA'SIRINI EKONOMETRIK BAHOLASH	12-22
<i>Dr. Abror Kucharov, Dr. Jyoti Meshram</i> COMPARATIVE ANALYSIS OF INDIAN INVESTMENT IN CENTRAL ASIA AND ITS RELEVANCE FOR UZBEKISTAN	23-32
<i>Qodirov Abubakr, Egamberdiyev Muzaffar</i> O'ZBEKISTON IQTISODIYOTINING TAYANCH HUDUDI: FARG'ONA VILOYATI VA UNING IQTISODIY TARMOQLARI	33-37

09.00.00 – FALSAFA FANLARI

<i>Tursunkulova Shaxnoza Tuychiyevna</i> TASAVVUF ESTETIKASIDA GO'ZALLIKNING TARBIYAVIIY POTENSIALI	38-43
--	-------

10.00.00 – FILOLOGIYA FANLARI

<i>Muxammadieva Mashxura, Amirqulova Gulxayo</i> TIBBIY TERMINOLOGIYANI O'QITISHDA ZAMONAVIIY PEDAGOGIK TEXNOLOGIYALARDAN FOYDALANISH	44-49
<i>Naimova Parvina Rustamovna</i> O'ZBEK TILIDA HAYVON OBRAZLARINING FRAZELOGIZMLARDA VA MAQOLLARDA INSON XARAKTERI VA XULQINI IFODA ETISHI	50-54
<i>Tashxujayeva Nigora Madaminjanovna</i> FRAZELOGIK BIRLIKLARDA MIFOLOGEMALARNING KOGNITIV-SEMANTIK TAHLILI	55-58

12.00.00 – YURIDIK FANLAR

<i>Zokirov Sherzod</i> MAHALLIIY DAVLAT HOKIMIYATI ORGANLARI QARORLARI QONUNIYLIGI USTIDAN PROKUROR NAZORATINI RAQAMLASHTIRISH MASALALARI	59-65
<i>Mirzaabdullayeva Matluba Rustamovna</i> YER SERVITUTINI RIVOJLANISHI	66-70
<i>Uzbekova Dilshoda Tulkinovna</i> ИСТОРИЯ И РАЗВИТИЕ ПРОЦЕССУАЛЬНОГО ПРИНУЖДЕНИЯ В УГОЛОВНОМ ПРОЦЕССЕ РЕСПУБЛИКИ УЗБЕКИСТАН	71-80

<i>Yo'ldoshev Ilhom Abdujalil o'g'li</i> KIBERKORRUPSION JINOYATLAR BO'YICHA AYRIM ILMIY-NAZARIY MULOHAZALAR	81-87
<i>Adizov Alibek Oybek o'g'li</i> ZARARNING TO'LIQ QOPLANISHI MUNOSABATI BILAN JINOYAT ISHLARINI SUDGACHA TUGATISH: NAZARIY VA AMALIY MASALALAR	88-94
<i>Xoligova Gavhar Ramazon qizi</i> CHET EL ELEMENTI BILAN MURAKKABLAHGAN ALIMENT MAJBURIYATLARINI TARTIBGA SOLISHNING NAZARIY HUQUQIY JIHATLARI	95-99
<i>Низомова Настарин Владимировна</i> МЕЖДУНАРОДНОЕ СОТРУДНИЧЕСТВО В СФЕРЕ КИБЕРБЕЗОПАСНОСТИ: СРАВНИТЕЛЬНЫЙ АНАЛИЗ ЯПОНИИ И УЗБЕКИСТАНА	100-107
13.00.00 – PEDAGOGIKA FANLARI	
<i>To'raeva Gulchiroy Sheralievna</i> RAQAMLI TA'LIM MUHITIDA BO'LAJAK MUHANDISLARNING TEXNOLOGIK KOMPETENTLIGINI RIVOJLANTIRISH	108-114
<i>Xodjayev Anvar Zakirovich</i> OG'IR ATLETIKADA DAST KO'TARISH MASHQINI BAJARISHGA O'RGATISH USLUBIYATI	115-125

Received: 31 August 2025
Accepted: 15 September 2025
Published: 30 September 2025

Article / Original Paper

INTERNATIONAL COOPERATION IN THE FIELD OF CYBERSECURITY: COMPARATIVE ANALYSIS OF JAPAN AND UZBEKISTAN

Nizomova Nastarin Vladimirovna,
University of World Economy and Diplomacy,
Faculty of International Law,
Department of International Law and Public-Law Disciplines,
bachelor student
E-mail: nizomovanastarin69@gmail.com

Scientific supervisor: Nugmanov Nugman Abdullaevich, Doctor of Law (LL.D.), Professor,
University of World Economy and Diplomacy

Abstract. The article analyzes Japan's experience in international cybersecurity cooperation and develops recommendations for lessons learned for Uzbekistan. The study focuses on the applicability of Japanese strategic approaches – institutionalization, cyber diplomacy, and capacity-building – within the context of Uzbekistan's digital transformation.

Keywords: cybersecurity, Japan, Uzbekistan, international cooperation, cyber diplomacy, digital transformation.

МЕЖДУНАРОДНОЕ СОТРУДНИЧЕСТВО В СФЕРЕ КИБЕРБЕЗОПАСНОСТИ: СРАВНИТЕЛЬНЫЙ АНАЛИЗ ЯПОНИИ И УЗБЕКИСТАНА

Низомова Настарин Владимировна,
Университет мировой экономики и дипломатии,
Факультет «Международное право»,
Кафедра «Международное право и публично-правовые дисциплины»,
студентка бакалавриата

Научный руководитель: Нугманов Нугман Абдуллаевич,
Университет мировой экономики и дипломатии, д.ю.н., профессор

Аннотация. В статье анализируется опыт Японии в сфере международного сотрудничества по кибербезопасности и разрабатываются рекомендации по извлекаемым урокам для Узбекистана. Исследование фокусируется на возможностях применения японских стратегических подходов – институционализации, кибердипломатии и сотрудничества – в контексте цифровой трансформации Узбекистана.

Ключевые слова: кибербезопасность, Япония, Узбекистан, международное сотрудничество, кибердипломатия, цифровая трансформация.

DOI: <https://doi.org/10.47390/SPR1342V5SI8Y2025N15>

Введение. В современную эпоху цифровая трансформация стала ключевым драйвером экономического роста и социального развития, однако она же порождает беспрецедентные по масштабу и сложности вызовы в сфере кибербезопасности. Для развивающихся государств, активно внедряющих цифровые технологии, как

Узбекистан, эти вызовы носят особенно острый характер, требуя не только создания надежных национальных систем защиты, но и интеграции в глобальную архитектуру кибербезопасности. В этом контексте международное сотрудничество становится не опцией, а стратегической необходимостью, позволяя перенимать передовой опыт, участвовать в выработке норм и совместно противостоять транснациональным киберугрозам.

Целью данной статьи является анализ японской модели международного сотрудничества в сфере кибербезопасности и выявление извлекаемых из нее уроков для Республики Узбекистан. Япония была выбрана в качестве объекта исследования как страна, которая, столкнувшись с серьезными кибервызовами, сумела разработать комплексную и эффективную стратегию, сочетающую укрепление национальной устойчивости с активной кибердипломатией и наращиванием потенциала партнеров. В работе исследуются институциональные, стратегические и дипломатические аспекты японского подхода, а также оценивается их потенциальная применимость в условиях цифровой трансформации Узбекистана.

Методология. Для достижения поставленной цели в данном исследовании был применен метод анализа научной литературы и обзора источников. Автором был систематизирован и проанализирован корпус академических публикаций, стратегических документов и отчетов международных организаций, посвященных вопросам кибербезопасности Японии и Узбекистана. Сравнительный анализ позволил выявить ключевые закономерности, диспропорции и точки корреляции в подходах двух стран. Этот метод обеспечил комплексное понимание эволюции японской киберстратегии, ее основных принципов и инструментов, а также дал возможность провести объективную оценку текущего состояния и перспектив развития международного киберсотрудничества Узбекистана на основе выявленных лучших практик.

Результаты. Анализ японского опыта в сфере международного сотрудничества по кибербезопасности может представлять ценный ресурс для Узбекистана, где цифровизация ускоренными темпами охватывает экономику, государственные институты и социальную сферу. Япония уже в начале 2000-х годов признала транснациональный характер киберугроз и выработала «японскую модель кибердипломатии», подчеркнув, что вызовы, с которыми она сталкивается, будут актуальны и для других стран в будущем [4, с. 50]. Данное исследование выявляет ключевые уроки и корреляции между стратегическими подходами Японии и текущими потребностями Узбекистана.

Результаты анализа показывают, что фундаментом японского успеха стало своевременное создание robust институциональной базы. Так, после кибератаки на Mitsubishi Heavy Industry в 2011 г. и резкого роста числа атак на государственные сети Токио сформировал Совет по политике информационной безопасности, а затем Национальный центр готовности к чрезвычайным ситуациям и стратегии в области кибербезопасности (NISC) [4, с. 51]. Этот опыт напрямую коррелирует с недавними шагами Узбекистана, где в 2022 году был принят закон «О кибербезопасности» и назначен профильный регулятор в лице Службы государственной безопасности [8]. Однако, как и в ранней японской модели, узбекский подход пока остается в

значительной степени реактивным и compliance-ориентированным, что указывает на необходимость эволюции в сторону более проактивной и централизованно-координируемой модели по образцу NISC.

Японский опыт демонстрирует четкую эволюцию от сугубо технических мер к комплексной стратегии, интегрирующей международное сотрудничество. Последовательное развитие стратегий 2006, 2009 и 2010 гг. отражает переход от превентивного подхода к системе, основанной на сотрудничестве государства, частного сектора и международных партнёров [6, с. 00159]. Вторая Национальная стратегия информационной безопасности 2009 г. поставила амбициозную задачу достижения лидерства в Азии и установления стандартов безопасности совместно с США и ЕС [4, с. 50]. Для Узбекистана это означает необходимость выхода за рамки национального законодательства и разработки внешнеполитического компонента своей киберстратегии, ориентированного на региональное лидерство в Центральной Азии.

Анализ выявляет, что международное сотрудничество является стержнем японской модели. Его engagement структурировано вокруг трех столпов: продвижение верховенства права в киберпространстве, развитие мер доверия (CBMs) и активное участие в наращивании потенциала [7]. Это не просто идеализм, а отражение стратегического видения Японии, направленного на укрепление либерального международного порядка (LIO) и противодействие авторитарным режимам [1, с. 5–7]. Япония активно развивает диалог с НАТО, участвует в учениях Cyber Coalition и сотрудничает с Центром киберобороны НАТО [6, с. 00159]. Для Узбекистана, интегрирующегося в мировое киберпространство, данный опыт подчеркивает необходимость институционализации многосторонних форматов сотрудничества, включая диалог с ЕС, НАТО (в рамках программы «Партнерство во имя мира»), ОБСЕ и ведущими азиатскими странами.

Особого внимания заслуживает глубина двустороннего сотрудничества Японии. Важным элементом является взаимодействие с США: регулярный «Japan-US Cyber Dialogue» (с 2013 г.), совместные рабочие группы по киберобороне и участие в учениях [6, с. 00159]. Партнерство с Австралией сфокусировано на критических технологиях, безопасности цепочек поставок и управлении данными [7]. Параллельно Япония расширила сотрудничество с АСЕАН и в 2014 г. приняла у себя конференцию Meridian Process [4, с. 52]. Текущие международные связи Узбекистана, такие как сотрудничество с Group-IB или обмен опытом с Венгрией, носят тактический и ad-hoc характер. Японский опыт учит, что Узбекистану необходимо трансформировать эти связи в стратегические, долгосрочные партнерства с четкими рамками, подобные диалогу Японии и США.

Корреляция исследований показывает, что японская киберстратегия успешна потому, что она является не изолированной security-политикой, а компонентом экономического государственного управления (economic statecraft). Её помощь в наращивании потенциала – это инструмент защиты собственных цепочек поставок и продвижения своих компаний. Узбекистан с его стратегией «Цифровой Узбекистан 2030», нацеленной на превращение страны в региональный IT-хаб [9], имеет схожие экономические амбиции. Следовательно, кибербезопасность должна быть

интегрирована в этот план не как затратная статья, а как фундаментальное требование для привлечения иностранных инвестиций и становления надежным партнером.

Японский опыт демонстрирует сложный подход к сдерживанию (*deterrence*), который выходит за рамки военных аналогий и включает четыре механизма: наказание, отказ, "переплетение" (*entanglement*) и нормы [5, с. 58]. При этом Япония придерживается оборонительной позиции, делая акцент на сдерживании за счет отказа (*deterrence by denial*) – повышения собственной киберустойчивости – и дипломатических инструментов, таких как публичная атрибуция атак и «*naming and shaming*» [3, с. 434;2]. Это особенно актуально для Узбекистана, который, обладая ограниченными ресурсами, может достигать сдерживания не через наступательные операции, а через мощную оборону, международную кооперацию и дипломатическое давление.

Японская стратегия сфокусирована на конкретных угрозах, исходящих от Китая и КНДР, что отражается в борьбе с хакерскими группами (например, АРТ 10) и защите критической инфраструктуры [6, с. 00159]. Аналогичным образом Узбекистану следует проводить оценку угроз, исходящих как от государственных, так и негосударственных акторов в регионе, и формировать систему «коллективной киберустойчивости» в сотрудничестве с партнёрами по Центральной Азии. Это соответствует японскому подходу «двойного следа» (*dual-track approach*), сочетающего укрепление собственных возможностей с использованием мер по укреплению доверия (CBMs) [3с. 434-435].

Не менее значимым уроком является внимание Японии к человеческому капиталу. В Стратегии 2013 г. одним из направлений стало развитие программ по подготовке специалистов, а также выработка этических кодексов [4, с. 53]. Совместные программы ЕС и Японии направлены на развитие потенциала в сфере технологий и подготовку специалистов, что отражает стратегическую ориентацию на долгосрочную устойчивость [7, с. 574]. Для Узбекистана, где вопросы цифровой грамотности и кадрового обеспечения остаются острыми, это указывает на приоритетность образовательных инициатив и программ обмена опытом в рамках международных партнерств.

Япония активно регулирует деятельность социальных сетей, что является частью обеспечения общей цифровой безопасности [4, с. 54]. Для Узбекистана, где социальные сети становятся ключевым каналом распространения информации и источником угроз дезинформации, полезным может быть изучение японских механизмов государственного и корпоративного контроля, основанных на прозрачных этических нормах.

Однако японский опыт также показывает, что международные инициативы имеют ограничения, связанные с расхождением стратегических приоритетов и ресурсами [1, с. 14–16]. Это актуально и для Узбекистана, которому требуется прагматичный баланс между национальными интересами, сотрудничеством с Западом, Россией и Китаем, избегая вовлечения в геополитические конфликты. Как и Япония, Узбекистан может использовать «многостороннюю дипломатию» для сохранения стабильности [3, с. 434-435].

Японский опыт подчеркивает важность международно-правового измерения цифровой безопасности: как отмечает Нугманов, глобальное информационное

пространство становится источником не только возможностей, но и новых угроз, требующих согласованного регулирования на уровне международных организаций [10, с. 40]. Для Узбекистана это означает необходимость развивать собственную нормативную базу в сфере кибербезопасности в увязке с международными соглашениями и стандартами, а также обеспечивать участие женщин и молодежи в формировании цифровой политики как фактора устойчивости. Такой подход позволит интегрировать национальные интересы в общий контекст региональной и глобальной киберустойчивости, минимизируя уязвимость перед трансграничными угрозами и усиливая позиции страны в международном диалоге.

Таким образом, проведенный корреляционный анализ различных исследований позволяет сделать вывод, что японский опыт предлагает Узбекистану не набор разрозненных практик, а целостную парадигму. Ключевой вывод заключается в том, что кибербезопасность должна рассматриваться не как сугубо техническая, но как комплексная дипломатическая и экономическая задача, требующая прочной институциональной базы, интеграции в международные сети сотрудничества и одновременного укрепления национального потенциала. Перенятие адаптированных японских практик позволит Узбекистану не только повысить устойчивость критической инфраструктуры, но и занять более активную позицию в формировании правил регионального киберпространства.

Обсуждение. Проведенный анализ позволяет выявить ключевые диспропорции в подходах Японии и Узбекистана к кибербезопасности и наметить пути трансформации текущей узбекской модели. Как иллюстрирует Таблица 1, если Япония демонстрирует зрелую, комплексную стратегию, где кибербезопасность является инструментом внешней политики и экономической государственности, то Узбекистан находится на начальном этапе этого пути, где кибербезопасность пока остается вторичным по отношению к цифровизации компонентом. Основным вызов для Узбекистана заключается в преодолении этого разрыва и интеграции вопросов безопасности в самую ткань своей цифровой трансформации.

Таблица 1 Сравнительный контекст кибербезопасности: Япония и Узбекистан

Стратегический элемент	Подход Японии (на основе анализа)	Текущий статус Узбекистана (на основе анализа)
Национальная стратегия	Зрелая, комплексная, проактивно-реактивная стратегия, рассматривающая кибербезопасность как инструмент внешней и оборонной политики.	Амбициозная, базовая стратегия «Цифровой Узбекистан 2030», где кибербезопасность является важным, но не полностью интегрированным компонентом.
Основной драйвер	Экономическая безопасность (защита цепочек поставок, поддержка компаний) является главным катализатором сотрудничества.	Быстрая цифровизация и экономический рост — основные драйверы, при этом кибербезопасность рассматривается как необходимое, но второстепенное направление.
Развитие потенциала	«Высоко ориентированный на безопасность» и системный подход, используемый для	Ад-хок, двусторонние и зачастую инициируемые частным сектором партнерства, направленные на

	защиты собственных цепочек поставок и укрепления региональной устойчивости.	восполнение конкретных технических и институциональных пробелов.
Международные партнёрства	Стратегические, долгосрочные взаимодействия (например, с АСЕАН, ЕС), направленные на достижение широких геополитических и экономических целей.	В основном двусторонние и технические, обслуживающие текущие потребности, а не более широкую, регионально ориентированную дипломатическую стратегию.

Ключевым направлением для такого стратегического скачка является переосмысление роли международного сотрудничества. В настоящее время партнерства Узбекистана носят тактический и ad-hoc характер, фокусируясь на двустороннем обмене опытом и технической помощи. Японский опыт учит, что *saracity-building assistance* (CBA) должен быть не просто помощью, а системным, «ориентированным на безопасность» инструментом внешней политики. Узбекистан, обладая развитой правовой базой и амбициями регионального IT-хаба, имеет все возможности для того, чтобы формализовать и масштабировать свои усилия, создав системную программу CBA для Центральной Азии. Это позволит стране позиционировать себя не как потребителя, а как поставщика кибербезопасности, приобретение престижа и влияния, подобно тому, как Япония делает это в Юго-Восточной Азии, трансформируя тем самым свои партнерства из разрозненных обменов в стратегический дипломатический актив.

Важнейшим уроком является также необходимость соблюдения баланса между проактивными и реактивными мерами. Япония выстроила свою стратегию на этом фундаментальном равновесии, где мощные системы реагирования дополняются упреждающей кибердипломатией и обменом разведанными. Узбекистан демонстрирует начальное понимание этого, как видно на примере политики управления международным интернет-трафиком, которая включает элементы проактивного контроля. Однако данный подход должен быть расширен на все инициативы в рамках «Цифрового Узбекистана-2030». Для каждого нового проекта критической инфраструктуры или электронного правительства разработка проактивного плана безопасности, включающего протоколы обмена информацией и модели публично-частного партнерства, должна быть обязательным требованием с самого начала, а не запоздалой реакцией на инцидент.

Наконец, Узбекистану необходимо сформулировать собственную нормативную позицию в глобальном киберпространстве. Япония искусно сочетает продвижение идеалов «свободного и открытого интернета» с прагматичными инструментами сдерживания, такими как публичная атрибуция атак. Для Узбекистана урок с нюансами заключается в том, что эти подходы не взаимоисключают, а дополняют друг друга. Страна может и должна активно продвигать кооперативные, основанные на развитии нормы в рамках ШОС и СНГ, одновременно развивая собственные возможности для атрибуции угроз и киберсдерживания для защиты своего суверенитета. Такой «двойной трек» позволит Узбекистану укрепить свой авторитет как ответственного

регионального лидера, одновременно гарантируя защиту национальных интересов в условиях растущих геополитических турбулентностей.

Заключение. Проведенное исследование демонстрирует, что японский опыт построения системы международного сотрудничества в сфере кибербезопасности предлагает Узбекистану ценные и многогранные уроки. Ключевой вывод заключается в том, что эффективная кибербезопасность в XXI веке достигается не только за счет технических мер, но и через прочную институциональную базу, интегрированную в экономическую стратегию, и активную внешнюю политику. Узбекистан, находясь на активной стадии цифровой трансформации, имеет уникальную возможность избежать этапа проб и ошибок, сразу внедряя комплексный подход, заимствованный из японской практики: от создания централизованного координационного центра по образцу NISC до развития стратегических, а не тактических, партнерств с ключевыми игроками.

Таким образом, перспективы для Узбекистана заключаются в переходе от роли потребителя международной технической помощи к роли поставщика кибербезопасности и регионального лидера в Центральной Азии. Для этого необходимо трансформировать текущие инициативы в системную программу наращивания потенциала, четко определить свою нормативную позицию в глобальном киберпространстве и сделать кибербезопасность неотъемлемым элементом своей экономической государственной политики. Реализация этих шагов позволит республике не только значительно повысить свою национальную устойчивость, но и занять влиятельную позицию в формировании региональных и глобальных правил игры в киберпространстве.

Литература/References/Adabiyotlar:

1. Atanassova-Cornelis E., Pejsova E. The EU-Japan security cooperation in defence of the liberal international order: achievements and limitations //Asia Europe Journal. – 2025. – С. 1-18.
2. Egloff, Florian J. 2020. "Public Attribution of Cyber Intrusions." Journal of Cybersecurity 6 (1): tyaa012. doi:10.1093/cybsec/tyaa012.
3. Manantan, Mark Bryan. 2020b. "Prospects for the Philippines-Japan-Australia Trilateral Cooperation." In Towards an Enhanced Strategic Policy in the Philippines, edited by A.Arugay, and H. Kraft. Konrad Adenauer Stiftung, and UP Center for Integrative Studies.
4. Melkonyan, Lusine. (2022). Japan's Approaches to International Cooperation in the Field of Cybersecurity: the Case of ASEAN. Problemy dalnego vostoka. 49. 10.31857/S013128120019300-1.
5. Nye, Joseph S. 2017. "Deterrence and Dissuasion in Cyberspace." International Security 41 (3): 44–71. doi:10.1162/ISEC_a_00266.
6. Ukhanova E. Cybersecurity and cyber defence strategies of Japan //SHS Web of Conferences. – EDP Sciences, 2022. – Т. 134. – С. 00159.
7. Vosse W. A conceptional broadening of the security order in the Indo-Pacific: The role of EU-Japan cooperation in ICT and cybersecurity //Asian Affairs. – 2022. – Т. 53. – №. 3. – С. 561-582.
8. Закон Республики Узбекистан «О кибербезопасности» от 15.04.2022 № LRU-764 // Dentons. — 22 апреля 2022. — Режим доступа: <https://www.dentons.com/en/insights/articles/2022/april/22/uzbekistan-adopts-cybersecurity-law>

9. Муйдинов Э. А. Перспективы цифрового Узбекистана 2030: развитие системы цифрового правительства // Web of Scholars Journal. – 2024. – Т. 2, № 7. – С. 12–18. – URL: <https://webofjournals.com/index.php/8/article/download/1647/1623/3224>
10. Нугманов Н.А. Международно-правовое регулирование сотрудничества в области международного обмена информацией // Вестник Поволжского института управления. №2 (47), 2015. Саратов. - С. 40. <http://vestnik.pags.ru/vestnik/archive/vestnik-47.php>

SCIENCEPROBLEMS.UZ

IJTIMOYIY-GUMANITAR FANLARNING DOLZARB MUAMMOLARI

№ 5/8 (5) – 2025

АКТУАЛЬНЫЕ ПРОБЛЕМЫ СОЦИАЛЬНО- ГУМАНИТАРНЫХ НАУК

ACTUAL PROBLEMS OF HUMANITIES AND SOCIAL SCIENCES

“Ijtimoiy-gumanitar fanlarning dolzarb muammolari” elektron jurnali 2020-yil 6-avgust kuni 1368-sonli guvohnoma bilan davlat ro'yxatiga olingan.

Muassis: “SCIENCEPROBLEMS TEAM”
mas'uliyati cheklangan jamiyati

Tahririyat manzili:

100070. Toshkent shahri, Yakkasaroy tumani, Kichik Beshyog'och ko'chasi, 70/10-uy. Elektron manzil:

scienceproblems.uz@gmail.com

Bog'lanish uchun telefon:

(99) 602-09-84 (telegram).