КИБЕРБЕЗОПАСНОСТЬ В ЦИФРОВЫХ КОНСУЛЬСКИХ УСЛУГАХ: ВЫЗОВЫ И ПРАВОВЫЕ ГАРАНТИИ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ ГРАЖДАН ЗА РУБЕЖОМ

Абдукаххорова Мохичехра Иззатилло кизи
Магистрант факультета практики и применения уголовного законодательства Ташкентского государственного юридического Университета
Ташкент, Узбекистан

CYBERSECURITY IN DIGITAL CONSULAR SERVICES: CHALLENGES AND LEGAL SAFEGUARDS FOR THE PROTECTION OF CITIZENS' PERSONAL DATA ABROAD

Abdukakhkorova Mokhichekhra Izzatillo kizi
Master's student of the Faculty of Practice and Application of Criminal Law
Tashkent State University of Law
Tashkent, Uzbekistan

Аннотация: Современная цифровизация оказывает глубокое влияние на международные отношения, дипломатическую практику и консульскую деятельность. Одним из центральных вызовов цифровой эпохи стало обеспечение кибербезопасности и защита персональных данных, в особенности в контексте трансграничного взаимодействия. В статье анализируются международно-правовые инструменты, такие как Конвенция Совета Европы о защите данных, Общий регламент ЕС по защите данных (GDPR), Будапештская конвенция о киберпреступности и резолюции ООН. Подчеркивается значение международной ответственности государств за утечку данных и киберпреступления, рассматриваются вызовы, включая технологическое неравенство, разнородность юрисдикции и угрозы правам человека в цифровом пространстве.

Abstract. Modern digitalization has a profound impact on international relations, diplomatic practice, and consular activities. One of the central challenges of the digital era is ensuring cybersecurity and protecting personal data, especially in the context of cross-border interactions. This article analyzes international legal instruments such as the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, the EU General Data Protection

Regulation (GDPR), the Budapest Convention on Cybercrime, and UN resolutions. It emphasizes the importance of state responsibility for data breaches and cybercrimes, and explores challenges including technological inequality, jurisdictional fragmentation, and threats to human rights in the digital space.

Ключевые слова: *кибербезопасность, международное право, персональные данные, GDPR, Будапештская конвенция, цифровая дипломатия, консульская деятельность, киберугрозы.*

Keywords: *cybersecurity, international law, personal data, GDPR, Budapest Convention, digital diplomacy, consular services, cyber threats.*

Цифровая трансформация затронула все аспекты современного мира, включая международные отношения, правовую систему и защиту прав граждан. Консульские службы, как важный канал взаимодействия между гражданами и государствами, все чаще полагаются на цифровые инструменты. Это обостряет вопросы обеспечения кибербезопасности и защиты персональных данных, особенно в условиях трансграничного правового взаимодействия.

Современные технологии позволяют в реальном времени обрабатывать и передавать огромные массивы данных, включая персональные. Однако это сопровождается ростом числа киберугроз, что требует от государств не только технологической адаптации, но и совершенствования международно-правового регулирования. Примером служит хакерская атака 15 июля 2020 года на аккаунты известных политиков и предпринимателей США в Twitter, что продемонстрировало, насколько уязвимыми могут быть даже глобальные цифровые платформы.

Первым крупным международным документом в этой сфере стала **Конвенция Совета Европы 1981 года**, установившая базовые принципы обработки персональных данных. Однако ключевым шагом стало принятие **GDPR** в Европейском союзе, который не только закрепил строгие нормы защиты, но и распространил их действие на организации за пределами ЕС. GDPR стал образцом для многих стран и компаний, а также важным инструментом привлечения к ответственности за нарушение прав на неприкосновенность личной информации.

Вопросы киберугроз регулируются Будапештской конвенцией о киберпреступности (2001), которая установила правовую базу для противодействия незаконному доступу к информационным системам, вмешательству в данные, распространению вредоносного ПО. Конвенция способствует обмену информацией между государствами, совместным расследованиям и экстрадиции киберпреступников.

Дополнительно, Резолюции Генеральной Ассамблеи ООН, в том числе по защите критической инфраструктуры и прав человека в цифровом пространстве, формируют международную повестку и подталкивают к формированию глобальных стандартов.

Несмотря на прогресс в международном правовом регулировании, остается множество проблем:

1. Отсутствие единых универсальных стандартов ведет к правовой фрагментации. На международной арене отсутствуют универсальные и обязательные для всех участников стандарты в области цифровых технологий, в том числе в аспекте защиты персональных данных и цифровой безопасности. Это приводит к возникновению множества разрозненных нормативно-правовых актов в разных странах, что затрудняет выработку общего подхода к регулированию цифрового пространства, в том числе в рамках консульской и дипломатической деятельности. Такая правовая фрагментация препятствует эффективному сотрудничеству между государствами и снижает правовую определенность в трансграничных вопросах.

2. Технологическое неравенство затрудняет реализацию международных соглашений в развивающихся странах. Многие развивающиеся государства не обладают достаточными техническими, финансовыми или кадровыми ресурсами для внедрения и соблюдения международных стандартов в сфере цифровых технологий. Это приводит к неравномерной реализации международных обязательств, нарушению принципа равноправия государств и снижению эффективности глобальных инициатив, включая те, что касаются защиты граждан за рубежом посредством цифровых инструментов.

3. Различия в юрисдикциях осложняют расследование и наказание киберпреступлений. Из-за существенных различий в уголовных и процессуальных законах, в определениях составов киберпреступлений и в порядке взаимодействия между правоохранительными органами, международное сотрудничество в расследовании киберпреступлений сталкивается с серьезными затруднениями. Это касается, в частности, дел, связанных с вмешательством в работу цифровых платформ, используемых для предоставления консульских услуг, а также незаконного доступа к персональным данным граждан.

4. Риски нарушения прав человека, в том числе права на неприкосновенность частной жизни, могут усиливаться под предлогом обеспечения безопасности. С развитием цифровых технологий возрастает возможность государств отслеживать действия пользователей, контролировать цифровые коммуникации и собирать персональные данные. Под предлогом

обеспечения национальной безопасности или предотвращения преступлений могут внедряться чрезмерные меры контроля, нарушающие базовые права человека, включая право на частную жизнь, свободу выражения мнений и защиту персональной информации. Это требует особого внимания к вопросам правовой регламентации, баланса интересов и обеспечения прозрачности в использовании цифровых инструментов, особенно в контексте виртуальной дипломатии и защиты прав граждан за границей.

Отсутствие единых универсальных стандартов в сфере цифровой дипломатии и кибербезопасности ведет к правовой фрагментации и усложняет международное сотрудничество. Технологическое неравенство между развитыми и развивающимися странами затрудняет реализацию международных соглашений и создает барьеры для эффективной защиты данных. Различия в юрисдикциях создают сложности в расследовании и привлечении к ответственности за киберпреступления, особенно если преступники действуют из-за границы. Кроме того, под предлогом обеспечения безопасности возрастают риски нарушения прав человека, в частности, права на неприкосновенность частной жизни. В этих условиях государства несут ответственность за происходящее на их территории: как за прямые утечки или неправомерную обработку персональных данных, так и за бездействие в обеспечении защиты информационной инфраструктуры. Также на них возлагается ответственность за киберпреступления, если они исходят с территории страны и игнорируются или даже поощряются властями.

Механизмы ответственности включают как международные судебные процедуры, так и санкционные меры, предусмотренные национальным и международным правом.

Международно-правовая ответственность государств за обеспечение кибербезопасности и защиту персональных данных становится ключевым элементом цифровой глобальной повестки. Необходима не только унификация стандартов, но и обеспечение эффективного международного сотрудничества, прозрачности и уважения прав человека. Разработка правовых норм должна учитывать быстро меняющийся характер угроз и обеспечивать адаптацию законодательства к новым цифровым вызовам.

Список использованной литературы

1. Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных от 28 января 1981 года. ETS № 108.
2. Общий регламент Европейского Союза по защите данных (General Data Protection Regulation, GDPR). Регламент (ЕС) 2016/679 от 27 апреля 2016 г.
3. Конвенция о киберпреступности (Будапештская конвенция) от 23 ноября 2001 года. ETS № 185.

4. Резолюция Генеральной Ассамблеи ООН A/RES/73/27 «Развитие в области информационных и телекоммуникационных технологий в контексте международной безопасности», 2018.
5. Резолюция Генеральной Ассамблеи ООН A/RES/68/167 «Право на неприкосновенность частной жизни в цифровую эпоху», 2013.
6. Хакерская атака на Twitter 15 июля 2020 года // BBC News. URL: https://www.bbc.com/russian/news-53428477 (дата обращения: 20.07.2025).
7. Шабанов А.В. Международно-правовое регулирование защиты персональных данных: современные вызовы и тенденции // Международное право и международные организации. 2022. № 2. С. 45–56.
8. Тураев Ш.Р. Цифровизация консульской деятельности: правовые и организационные аспекты // Юридическая наука и практика. 2023. № 4. С. 102–109.
9. Бабаев Х.Б. Международная правовая ответственность государств за киберпреступления // Журнал зарубежного законодательства. 2021. № 3. С. 89–95.
10. Касымов У.Ю. Цифровая дипломатия и защита прав граждан за рубежом в условиях цифровой трансформации // Право и инновации. 2023. № 1. С. 67–73.
11. Council of Europe. Convention 108+ for the Protection of Individuals with regard to Processing of Personal Data. URL: https://www.coe.int/en/web/data-protection/convention108-plus (accessed: 20.07.2025).
12. United Nations. Human Rights in the Digital Age. UN Human Rights Office. URL: https://www.ohchr.org/en/digital-space (accessed: 20.07.2025).
13. European Commission. Data Protection Rules as a Trust-Enabler in the EU and Beyond. URL: https://ec.europa.eu/info/law/law-topic/data-protection_en (accessed: 20.07.2025).
14. International Telecommunication Union. Global Cybersecurity Index 2021. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx (accessed: 20.07.2025).