

Глобальные вызовы и международные документы в сфере информационной безопасности

Научный руководитель – Емельянович Ольга Викторовна

Логвинов Павел Дмитриевич

Студент (бакалавр)

Белорусский государственный университет, Юридический факультет, Минск, Беларусь

E-mail: logvinovpd@yandex.ru

Современный мир переживает эпоху цифровой трансформации, которая затрагивает все сферы человеческой жизни — от экономики и политики до социальных отношений и культуры. Информационные технологии стали неотъемлемой частью глобальной инфраструктуры, обеспечивая развитие и взаимодействие государств, бизнеса и общества. Однако вместе с возможностями цифровизации возникают и новые вызовы, связанные с обеспечением информационной безопасности. Киберугрозы, такие как кибератаки, утечки данных, распространение вредоносного программного обеспечения и использование цифровых технологий в преступных целях, приобретают транснациональный характер, что требует скоординированных усилий на международном уровне.

Одним из свежих примеров крупного взлома является ситуация, связанная с криптобиржей Bybit. 21 февраля 2025 года хакеры украли порядка 1.5 миллиарда долларов в криптовалюте Ethereum, использовав сложный метод подмены транзакции, который позволил получить им полный доступ к определенной части активов. В связи со случившемся, многие пользователи, а также инвесторы стали обеспокоены сложившемся положением дел. Данный пример служит напоминанием о необходимости укрепления международной правовой базы для обеспечения информационной безопасности [12].

Для понимания проблематики данной темы, требуется привести следующее определение:

- “информационная безопасность - состояние защищенности личности, общества и государства и их интересов от угроз, деструктивных и иных негативных воздействий в информационном пространстве” [5].

Мы согласны с мнением Данеляна А.А. и Гуляевой Е.Е., что в современном мире требуется универсализация существующего международно-правового регулирования применительно к киберпространству с учетом его определенной специфики и в целях эффективного правового противодействия использованию информационно-коммуникационных технологий в незаконных целях [6].

Создание механизма обеспечения информационной безопасности на международной арене необходимо в целях защиты национальных экономик и граждан. Это возможно благодаря слаженной работе государства с ведущими специалистами в сфере информационной безопасности, экономики, международных экономических отношений [1].

Учитывая необходимость универсализации международно-правового регулирования в киберпространстве и создания эффективных механизмов обеспечения информационной безопасности, важно обратить внимание на ключевые угрозы, с которыми сталкивается современное цифровое пространство, а также на правовые решения, способные минимизировать эти риски.

В условиях стремительного развития информационно-коммуникационных технологий и их активного использования в незаконных целях, выделяются следующие основные угрозы:

- 1) Кибератаки на критическую инфраструктуру;
- 2) Утечки данных и нарушение приватности;
- 3) Криптопреступность и отмывание денег;
- 4) Дезинформация и киберпропаганда;
- 5) Использование ИИ для кибератак.

Для противодействия этим вызовам международное сообщество и отдельные государства разрабатывают и внедряют следующий комплекс правовых мер:

- Конвенция о компьютерных преступлениях №185, 23 ноября 2001 года [3];
- Директива 2022/2555 О мерах по обеспечению высокого общего уровня кибербезопасности во всем Союзе от 14 декабря 2022 года [8];
- Общий регламент защиты персональных данных Европейского союза (GDPR) [11];
- Рекомендации ФАТФ: Международные стандарты по противодействию отмыванию денег, финансированию терроризма и финансированию распространения оружия массового уничтожения [2];
- Директива (ЕС) 2018/843 О внесении изменений в Директиву (ЕС) 2015/849 ЕВРОПЕЙСКОГО ПАРЛАМЕНТА И СОВЕТА ЕС о предотвращении использования финансовой системы в целях отмывания денег или финансирования терроризма от 30 мая 2018 года [9];
- Рекомендация об этических аспектах искусственного интеллекта ЮНЕСКО от 24 ноября 2021 года [4];
- Рамочная конвенция Совета Европы об искусственном интеллекте и правах человека, демократии и верховенстве закона №225 от 5 сентября 2024 г. [7];

18 ноября 2024 года Совет Европейского союза принял Декларацию об общем Понимании применения международного права в киберпространстве. В данной декларации было разъяснено, что международное право, в частности Устав ООН, международное право прав человека и международные гуманитарное право в полной мере применимо и к киберпространству [10]. Данная Декларация подтверждает применимость международного права в киберпространстве, что имеет ключевое значение для его регулирования.

Современные киберугрозы, такие как взломы, утечки данных и криптопреступность, требуют конкретных мер реагирования со стороны международного сообщества. Описанные выше международно-правовые решения демонстрируют важность глобального сотрудничества. Защита критической инфраструктуры, приватности и борьба с дезинформацией возможны только через строгое регулирование и координацию между государствами, организациями и бизнесом. Укрепление международной правовой базы — необходимое условие для обеспечения безопасности в эру цифровых технологий.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

- 1) Юдина Ю.А. Возможность применения средств обеспечения международной безопасности к информационному пространству // Актуальные проблемы российского права, 2022. № 6. С. 168–176.
- 2) Рекомендации ФАТФ: Международные стандарты по противодействию отмыванию денег, финансированию терроризма и финансированию распространения оружия массового уничтожения / Пер. с англ. — М.: МУМЦФМ, 2012. — 196 с.

- 3) Конвенция о компьютерных преступлениях Совет Европы, Будапешт, 23.11.2001 года.
- 4) Рекомендация ЮНЕСКО: Об этических аспектах искусственного интеллекта / Пер. с англ. — 2021. — 21 с.
- 5) Решение о Стратегии обеспечения информационной безопасности государств - участников Содружества Независимых Государств, г.Москва, 25 октября 2019 года.
- 6) Danelyan A.A., Gulyaeva E.E. International Legal Aspects of Cybersecurity. - Moscow Journal of International Law. 2020. № 1. С. 44-53.
- 7) Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law / CETS No. 225. Vilnius, 05 September 2024.
- 8) Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).
- 9) Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU.
- 10) Declaration on a Common Understanding of International Law in Cyberspace / General Secretariat of the Council To: Delegations Brussels, 18 November 2024.
- 11) General Data Protection Regulation (EU GDPR) OJ L 127, 23.5.2018, p. 2 ((EU) 2016/679).
- 12) ПБК: <https://www.rbc.ru/crypto/news/67b8a3e19a79475d9effecf6>.