

Международное сотрудничество республики Беларусь в сфере информационных технологий и кибербезопасности

Актуальность международного взаимодействия государств в сфере цифровой безопасности обусловлена тем, что информационные технологии проникают во все сферы общественной жизни и играют ключевую роль в функционировании современного общества. Достижения технологического прогресса все активнее вовлекаются в глобализационные процессы, поэтому вопросы кибербезопасности и международной информационной безопасности становятся значимым направлением мировой политики. Международные отношения приобретают новую динамику, поскольку цифровая среда становится не только пространством сотрудничества, но и источником новых рисков, вызовов и угроз.

Международная информационная безопасность в белорусской внешнеполитической практике рассматривается как важное направление сотрудничества государств в целях противодействия преступным, террористическим и военно-политическим угрозам в информационном пространстве [1]. В этом контексте особое значение приобретают защита критически важной инфраструктуры, предупреждение кибератак, противодействие использованию информационно-коммуникационных технологий в противоправных целях, а также выработка международных правил ответственного поведения государств в киберпространстве.

Исследования Международного союза электросвязи при ООН показывают, что государства по всему миру усиливают меры по обеспечению кибербезопасности. Для оценки национальных усилий в этой сфере используется Global Cybersecurity Index, который анализирует уровень обязательств и практических мер государств по пяти направлениям: правовому, техническому, организационному, кадровому и международному [2].

В Global Cybersecurity Index 2024 уровень кибербезопасности Республики Беларусь был оценен как Tier 3 – Establishing. В данной методологии Tier 1 является наивысшим уровнем, а Tier 5 – низшим [2; 3]. Методология рейтинга включает 83 показателя, объединенных в пять основных групп. Оценка по каждой группе позволяет выявить сильные стороны национальной системы кибербезопасности и направления, требующие дальнейшего развития.

Показатели Беларуси распределились следующим образом при максимуме 20 баллов в каждой категории:

- юридические аспекты – 18,61;
- технические меры – 2,78;
- организационные стратегии – 11,97;
- развитие потенциала – 8,98;
- международное сотрудничество – 19,11 [3].

Данные показатели свидетельствуют о том, что у Республики Беларусь достаточно сильные позиции в сфере правового регулирования и международного сотрудничества. Вместе с тем низкая оценка по техническим мерам, а также умеренные показатели по организационным стратегиям и развитию потенциала указывают на необходимость дальнейшего совершенствования практических механизмов киберзащиты, подготовки кадров и институциональной координации.

Дополнительным фактором, влияющим на развитие цифровой безопасности Беларуси, выступает санкционное давление. В 2025 г. Европейский союз принял новые ограничительные меры в отношении Беларуси, включая ограничения в цифровой и технологической сферах [4; 5]. В частности, были введены меры, касающиеся программного обеспечения, связанного с разведкой нефти и газа, а также программных решений для управления предприятиями и промышленного проектирования, предназначенных для государственных органов, организаций и структур Беларуси [4].

Возникшая необходимость перехода на альтернативные программные решения усиливает значение импортозамещения, развития отечественных ИТ-продуктов и поиска надежных технологических партнеров. В этих условиях Беларусь и Россия расширяют сотрудничество в сфере цифровизации и программного обеспечения. Так, в 2025 г. было объявлено о сотрудничестве ОАО «Гипросвязь» и российской компании ООО «РусБИТех-Астра», направленном на развитие белорусско-российских отношений в сфере цифровизации, поддержку цифровой индустрии, обмен опытом и подготовку совместных рекомендаций по импортозамещению программного обеспечения [6].

Такое сотрудничество может способствовать снижению зависимости от западных программных решений, развитию национальных компетенций и укреплению технологической устойчивости. Одновременно важно учитывать, что импортозамещение само по себе не решает всех задач цифровой безопасности. Для устойчивого развития необходимы системная защита критической инфраструктуры, подготовка специалистов, регулярный аудит информационных систем, повышение цифровой грамотности пользователей и развитие собственных исследовательских и производственных возможностей.

Значимым направлением остается и международное сотрудничество в сфере выработки общих правил поведения в цифровой среде. Республика Беларусь заявляет о готовности развивать партнерские отношения в области международной информационной безопасности и поддерживать инициативы, направленные на формирование ответственного поведения государств в киберпространстве [1]. Такой подход позволяет рассматривать цифровую безопасность не только как техническую задачу, но и как элемент внешней политики, национальной безопасности и международной стабильности.

Таким образом, международное взаимодействие государств в сфере цифровой безопасности приобретает все большее значение. Для Республики Беларусь ключевыми задачами являются укрепление технической составляющей

кибербезопасности, развитие кадрового потенциала, совершенствование организационных механизмов, импортозамещение критически важных программных решений и участие в международном диалоге по вопросам ответственного поведения в цифровой среде. Решение этих задач позволит повысить устойчивость национальной цифровой инфраструктуры и укрепить позиции Беларуси в системе международной информационной безопасности.

Список источников

1. Международная информационная безопасность [Электронный ресурс] // Министерство иностранных дел Республики Беларусь. – Режим доступа: https://www.mfa.gov.by/multilateral/global_issues/inform/. – Дата доступа: 09.06.2026.
2. Global Cybersecurity Index 2024 : 5th edition [Electronic resource] / International Telecommunication Union. – Geneva : ITU, 2024. – Mode of access: https://www.itu.int/dms_pub/itu-d/opb/hdb/d-hdb-gci.01-2024-pdf-e.pdf. – Date of access: 09.06.2026.
3. Беларусь получила уровень Tier 3 в Global Cybersecurity Index 2024 [Электронный ресурс] // Noventiq Belarus. – 2024. – 24 сент. – Режим доступа: <https://noventiq.by/about/news/belarus-poluchila-uroven-tier-3-v-global-cybersecurity-index-2024>. – Дата доступа: 09.06.2026.
4. Council Regulation (EU) 2025/392 of 24 February 2025 amending Regulation (EC) No 765/2006 concerning restrictive measures in view of the situation in Belarus and the involvement of Belarus in the Russian aggression against Ukraine [Electronic resource] // EUR-Lex. – Mode of access: <https://eur-lex.europa.eu/eli/reg/2025/392/oj/eng>. – Date of access: 09.06.2026.
5. EU sanctions against Belarus [Electronic resource] // European Council ; Council of the European Union. – Mode of access: <https://www.consilium.europa.eu/en/policies/sanctions-against-belarus/>. – Date of access: 09.06.2026.
6. Беларусь и Россия вместе займутся импортозамещением ПО [Электронный ресурс] // Министерство связи и информатизации Республики Беларусь. – 2025. – 5 марта. – Режим доступа: <https://www.mpt.gov.by/ru/belarus-i-rossiya-vmeste-zaymutsya-importozamescheniem-po-0>. – Дата доступа: 09.06.2026.

***В.А. Моспанова, М.Д. Вороник, студенты ФЭМ**
Научный руководитель – А.А. Авангард*

Цифровой активизм: феминистские движения в эпоху социальных сетей. Современные платформы для борьбы за права женщин

Эпоха цифровизации существенно изменила формы общественного взаимодействия и протестной активности. Сегодня социальные сети являются