

Секция 14

ПОЛИТИЧЕСКИЕ ПРОБЛЕМЫ СОЦИАЛЬНО-ЭКОНОМИЧЕСКОГО РАЗВИТИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

В. И. Краевская

*Научный руководитель — кандидат политических наук К. И. Костиневич
БГЭУ (Минск)*

КИБЕРБЕЗОПАСНОСТЬ КАК СФЕРА НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

В современном мире информация — мощный стратегический ресурс. Экономический, оборонный и политический потенциал любой страны напрямую зависят от уровня развития ее информационной инфраструктуры. Информационная безопасность выходит на первый план, становясь ключевым элементом национальной безопасности в целом. Кибербезопасность (или безопасность киберпространства) определяется как сохранение конфиденциальности, целостности и доступности информации в киберпространстве.

Вопросы кибербезопасности стали неотъемлемой частью внешней политики государства в начале 2000-х гг. Так, в рамках развития обороны США было уделено особое внимание кибероперациям, признавая киберпространство новой областью противоборства. Стратегия национальной безопасности США и национальная стратегия в области кибербезопасности 2022 и 2023 гг. отражают важность информационной безопасности, а также интеграцию компьютерных сетей в системы управления [1, 2].

В Республике Беларусь в последние годы не оставляют без внимания безопасность в киберпространстве. На начало 2023 г. зафиксировано 15,7 тыс. киберпреступлений, для сравнения, в 2022 г. — 14,8 тыс. за этот же период [4]. Рост киберпреступности в Беларуси обусловлен увеличением доли безналичных расчетов, количества электронных устройств и финансовых операций, а также коли-

чества владельцев банковских карт и интернет-пользователей. В свою очередь, низкая осведомленность о законах информационной безопасности и отсутствие интереса населения к повышению этой грамотности создают благоприятную среду для киберпреступлений. В 2020 г. произошла серия кибератак на государственные учреждения и ресурсы силовых структур. Череда подобных событий демонстрировала явные уязвимые места национальной безопасности Беларуси.

На сегодняшний день осуществляется ряд программ и разработок развития укрепления кибербезопасности Беларуси. Основой для продвижения таких направлений стала поддержка президентом Беларуси этого актуального вопроса. 14 февраля 2023 г. А. Г. Лукашенко подписал Указ № 40 «О кибербезопасности», который вводит новую правовую основу для защиты национальной информационной инфраструктуры от угроз [5]. Система обеспечения кибербезопасности включает в себя оперативно-аналитический центр, национальный центр и центры кибербезопасности инфраструктуры.

Таким образом, на сегодняшний день кибербезопасность является важным аспектом обороноспособности любого государства. С нашей точки зрения, Республике Беларусь необходимо продолжать развиваться в направлении обеспечения кибербезопасности. Однако стоит отметить, что по-прежнему центральным остается вопрос кадров.

Источники

1. Biden-Harris Administration's National Security Strategy [Electronic resource] // The White House. — Mode of access: <https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf>. — Date of access: 10.03.2024.
2. National Cybersecurity Strategy. March 2023 [Electronic resource] // The White House. — Mode of access: <https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf>. — Date of access: 10.03.2024.
3. В Беларуси с начала 2023 года зафиксировано 15,7 тыс. киберпреступлений [Электронный ресурс] // БелТА. — Режим доступа: <https://belta.by/society/view/v-belarusi-s-nachala-2023-goda-zafiksirovano-157-tys-kiberprestuplenij-605224-2023/>. — Дата доступа: 10.03.2024.
4. О кибербезопасности Указ [Электронный ресурс] : № 40 от 14 февраля 2023 г. // Официальный интернет-портал Президента Республики Беларусь. — Режим доступа: <https://president.gov.by/ru/documents/ukaz-no-40-ot-14-fevralya-2023-g>. — Дата доступа: 10.03.2024.