М. А. Жигалкина, Е. С. Чебутаева, М. С. Шпак
БГЭУ (Минск)
*Научный руководитель — **О. А. Касабуцкая***

КИБЕРПРЕСТУПНОСТЬ КАК СИСТЕМНЫЙ ВЫЗОВ ДЛЯ РАЗВИТИЯ ЭЛЕКТРОННОЙ КОММЕРЦИИ В ИНТЕГРАЦИОННОМ ПРОСТРАНСТВЕ РОССИИ И БЕЛАРУСИ

Киберпреступность представляет серьезную угрозу национальной безопасности для экономик многих стран. Для анализа ее уровня в Союзном государстве использованы статистические данные, собранные группой ученых под руководством специалистов Оксфордского университета. На основе исследований разработан Всемирный индекс киберпреступности (WCI) и выделены 5 ключевых категорий киберпреступлений. Показатели по странам представлены в таблице.

Показатели уровня киберпреступности [1]

Показатели	Страны — участницы Союзного государства	
	Беларусь	Россия
Воздействие	6,84	8,96
Профессионализм	7,2	8,81
Технические навыки	7,32	8,73
Всемирный индекс киберпреступности (WCI)	3,87	58,39
Технические продукты/услуги	11,92	82,17
Атаки и вымогательство	5,58	81,34
Кража данных/идентификационных данных	1,85	65,18
Мошенничество	—	21,7
Обналичивание/отмывание денег	—	41,56

Как видно из таблицы, показатели Российской Федерации значительно превышают значения критериев Республики Беларусь. Этому могут способствовать несколько ключевых факторов: более ускоренная цифровизация экономики России, политизированность кибератак, а также повышенная монетизация в случае успеха киберпреступлений. Однако некоторые высокие значения критериев «профессионализм», «технические навыки» и «технические продукты» интерпретируются положительно, указывая на наличие высококвалифицированных кадров, обладающих значительным опытом в области ИТ. Для того чтобы подтвердить или опровергнуть данную гипотезу в дальнейшем, авторы индекса нацелены изучать также уровень образования, объем ВВП по странам, коррупцию и другие данные.

Анализируя показатели Республики Беларусь, можно отметить, что в целом показатели принимают умеренные значения. Наблюдается невысокий WCI. Явной специализацией страны является разработка ПО для отражения киберпреступлений, о чем свидетельствует высокое значение индекса «технические продукты/услуги». Очевидной проблемой является категория «атаки и вымогательство». В качестве меры реагирования целесообразно повысить уровень осведомленности населения о возможных рисках киберпреступности.

Таким образом, проведенное исследование позволило рассмотреть уровень киберпреступности в Республике Беларусь и Российской Федерации. Согласно международным оценкам российские киберпреступники признаются одними из наиболее технически оснащенных в мире. Беларусь же занимает 12-е место из топ-15. Обе страны активно развивают правовое поле, о чем свидетельствует Договор о противодействии легализации преступных доходов, подписанный 5 февраля 2025 г.

Источник

1. Mapping the global geography of cybercrime with the World Cybercrime Index / M. Bruce, J. Lusthaus, Ridhi Kashyap [et al.] // PLOS One. — URL: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0297312 (date of access: 14.11.2025).

Диплом «Признание» по итогам работы секции
М. В. Жуков
БГЭУ (Минск)
*Научный руководитель — **Л. С. Климченя**, канд. экон. наук, доцент*

ВОЗМОЖНОСТИ И РИСКИ ПРИМЕНЕНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ЭЛЕКТРОННОЙ КОММЕРЦИИ

Искусственный интеллект (далее ИИ) — технология, которая имитирует человеческое поведение, чтобы выполнять задачи и обучаться, используя собираемую информацию [1]. В сфере электронной коммерции ИИ становится ключевым драйвером трансформации бизнес-процессов.

Очевидно, что целью внедрения ИИ в электронную коммерцию является не только автоматизация рутинных операций, но и создание принципиально нового клиентского опыта, повышение конверсии и оптимизация логистических цепочек. Однако, как и в случае с любыми инновациями, использование ИИ требует значительных инвестиций и перестройки организационной структуры. Технологии