УДК 338.24(476)

Баранов А.М.
кандидат экономических наук, доцент,
доцент кафедры экономической теории
и мировой экономики учреждения образования
«Гомельский государственный университет им. Ф. Скорины»,
г. Гомель, Республика Беларусь

РИСКИ И УГРОЗЫ ЦИФРОВИЗАЦИИ, ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РЕСПУБЛИКИ БЕЛАРУСЬ

В статье исследуется проблема цифрового неравенства как ключевого вызова информационной безопасности современной экономической системы. Рассматривается эволюция концепции цифрового неравенства, включая его трехуровневую структуру (разрыв в доступе, навыках и результативности), предложенную в работах Л. Робинсон, Ш.Р. Цоттен, Х. Оно, А. Куан-Хаасе, Г.Месч, В.Чен, Й. Счулз, Т. М. Хале, М. Й. Стерн, Я.В. Дейка и др. Анализируются социально-экономические, антропогенные и психологические детерминанты цифрового расслоения, а также его влияние на формирование антропогененого капитала в контексте теорий П. Бурдье, М. Грановеттера и А.Портеса. Предложены институциональные меры по усилению роли высшего образования в преодолении цифрового неравенства в рамках практической реализации концепции «Образование 2.0». Исследованы глобальные проблемы кибербезопасности, включая рост сложности угроз (атаки с использованием ИИ, социальная инженерия), дефицит кадров и необходимость международной координации. Рассмотрены меры Беларуси по обеспечению цифрового суверенитета, включая сотрудничество с Россией в рамках Союзного государства и ЕАЭС, а также вызовы, связанные с технологической изоляцией и санкционным давлением недружественных стран. Определена необходимость комплексного подхода обеспечения информационной безопасности, сочетающего технологические, образовательные и институциональные решения для устойчивого развития информационной экономики Республики Беларусь.

Ключевые слова: цифровое неравенство, информационная безопасность, киберугрозы, цифровой суверенитет, человеческий капитал, высшее образование, Республика Беларусь.

A.M. Baranov

Candidate of Economic Sciences, Docent of Economy,

Associate Professor,

Department of Economic Theory and the world economy

Francisk Skorina Gomel State University

Gomel, Republic of Belarus

RISKS AND THREATS OF DIGITALIZATION: CHALLENGES OF ENSURING INFORMATION SECURITY IN THE REPUBLIC OF BELARUS

The article examines the problem of digital inequality as a key challenge to the information security of the modern economic system. It explores the evolution of the concept of digital inequality, including its three-tier structure (access gap, skills gap, and outcome gap), as proposed in the works of L. Robinson, S. R. Cotten, H.Ono, A.Quan-Haase, G.Mesch, W.Chen, M. J.Stern, J.V. Dijk and others. The study analyzes the socioeconomic, anthropogenic, and psychological determinants of digital stratification, as well as its impact on the formation of human capital in the context of theories by P. Bourdieu, M.Granovetter, and A. Portes.

Institutional measures are proposed to enhance the role of higher education in overcoming digital inequality through the practical implementation of the "Education 2.0" concept. The study investigates global cybersecurity challenges, including the increasing complexity of threats (AI-driven attacks, social engineering), workforce shortages, and the need for international coordination.

The article examines Belarus' efforts to ensure digital sovereignty, including cooperation with Russia within the framework of the Union State and the Eurasian Economic Union (EAEU), as well as the challenges posed by technological isolation and sanctions pressure from unfriendly states. The necessity of a comprehensive approach to information

security, combining technological, educational, and institutional solutions for the sustainable development of Belarus' information economy is emphasized.

Keywords: digital inequality, information security, cyber threats, digital sovereignty, human capital, higher education, Republic of Belarus.

Введение. Современная экономическая система, трансформирующаяся под влиянием цифровых технологий, сталкивается с рядом фундаментальных вызовов, среди которых особое место занимает проблема цифрового неравенства. Данный феномен, изначально рассматривавшийся как разрыв в доступе к информационно-коммуникационным технологиям (ИКТ), эволюционировал в сложную многоуровневую структуру, включающую неравенство в цифровых навыках и социально-экономических результатах использования технологий. В условиях глобальной цифровизации цифровое неравенство становится не только барьером для инклюзивного развития, но и угрозой информационной безопасности, поскольку формирует уязвимые группы населения, экономические субъекты и даже целые регионы, неспособные эффективно противостоять киберугрозам.

Одновременно с этим растет масштаб и сложность киберугроз, направленных на дестабилизацию государственных и экономических систем, что требует усиления мер по обеспечению цифрового суверенитета. Укрепление цифрового суверенитета становится необходимым условием для защиты национальных интересов, обеспечения устойчивого развития и безопасности информационной инфраструктуры Республики Беларусь в условиях усиливающейся глобальной конкуренции и геополитических рисков. Преодоление цифрового неравенства и противодействие киберугрозам выступают взаимодополняющими задачами, критически важными для формирования надежной и безопасной цифровой среды.

Основная часть. Одной из наиболее значимых проблем обеспечения информационной безопасности новой экономической системы является проблема цифрового неравенства. Цифровое неравенство – феномен комплексный и многомерный, находящийся в центре современных исследований информационного общества и новой экономики. Первоначально Организация по экономическому сотрудничеству и развитию (ОЭСР) определила цифровое неравенство как неравенство между отдельными лицами, домашними хозяйствами, предприятиями и географическими районами, находящимися на разных уровнях социально-экономического развития в отношении их возможностей доступа к ИКТ и Интернету для осуществления широкого спектра видов деятельности [1].

Со временем взгляды на цифровое неравенство претерпели эволюцию. Так в рамках исследования *Л. Робинсон, Ш.Р. Цоттен, Х. Оно, А. Куан-Хаасе, Г.Месч, В.Чен, Й. Счулз, Т.М. Хале, М.Й. Стерн* модель цифрового неравенства приобрела трехуровневую структуру [2].

Разрыв первого уровня (access gap) – неравенство в техническом доступе и инфраструктуре. Вследствие экономического неравенства, региональных различий, возрастного фактора и других детерминант формируются группы населения с разным уровнем доступа к ИТ. Данное расслоение получило научное обоснование в исследованиях профессора коммуникативных наук в университете Твенте *Я.В. Дейка*, который подчеркивает, что первым уровнем цифрового неравенства является физический доступ в сеть Интернет [3].

По мнению экспертов Всемирного банка и ООН доступ в Интернет, является неотъемлемой частью прав человека. По состоянию на начало 2025 года в мире только 5,56 млрд жителей (68% населения Земли) могли выходить во Всемирную сеть [4]. Это отправная точка цифрового неравенства. *Я.В. Дейк* полагает, что проблема неравенства никогда не будет решена, учитывая, что ряд стран уже находится на пути к широкому

внедрению мобильного Интернета 5G, ИИ, виртуальной реальности и других технологий нового уклада, а у трети населения Земли нет базового доступа в Интернет [3].

Разрыв второго уровня (skills gap) – различия в цифровых навыках, компетенциях и практиках использования технологий. Цифровое неравенство на данном уровне обусловлено не только техническими аспектами, но и психологическими, мотивационными факторами, уровнем образования и культурной средой. Так, по мнению *Дж. Ван Дейка* когда все население мира получит доступ к Интернету, неравенство цифровых навыков и умение пользоваться данными останется и, напротив, продолжит расти [3].

Разрыв третьего уровня (outcomes gap) – социально-экономические последствия использования цифровых технологий: доходы, образование, здоровье, участие в общественной жизни. Расширение использования сети Интернет и цифровых сервисов не гарантирует равных выгод для всех, что определено в исследованиях по «цифровому расслоению» [5]. Так, в социологии цифровое неравенство рассматривают как новый модус социальной дифференциации, связанный с неравенством в доступе к социальным благам и возможностям, порождаемым цифровой средой [6].

Психологический аспект, в частности различие в цифровых компетенциях разных поколений нашел отражение в *теории принятия технологий*, а также *теории мотивированного действия и теории запланированного поведения,* которые применяются для объяснения мотивации использования ИКТ и цифровых сервисов.

Цифровое неравенство непосредственно влияет на формирование антропогенного капитала – критического фактора экономического роста, что согласуется с исследованиями *П.Бурдье* [7], акцентирующего внимание в своих исследованиях на репродукции социального неравенства через социальный капитал, а также М.Грановеттера [8], Х.Флэпа [9] и

А.Портеса [10], Важнейшее значение приобретают исследования цифрового неравенства в сфере высшего образования, которое служит базой формирования ключевых цифровых компетенций, финансовой грамотности и профессиональных навыков.

Цифровое неравенство проявляется не только в доступе к цифровым ресурсам, но и в качестве их использования, а также в конечных образовательных эффектах, причем такие различия можно наблюдать между различными вузами, их подразделениями, преподавателями и студентами.

По справедливому замечанию *М.Д. Hanco* «Важную роль в формировании цифрового неравенства играют цифровые разрывы – между индивидами, группами индивидов, и чем сильнее эти барьеры, тем сложнее процесс их преодоления. В обществе, в котором средние классы не сформированы, а пространство низших классов достаточно обширно, возникают условия, которые усиливают цифровое неравноправие. Студенты из средних низших и низших слоев имеют меньше финансовых и материальных возможностей для успешной интеграции в цифровой контекст, что отражается на качестве получаемого высшего образования» [11].

Для эффективного преодоления цифрового неравенства в современном высшем образовании необходим *системный и комплексный подход*, ключевым элементом которого является развитие Образования 2.0. Данный подход предполагает не просто внедрение цифровых технологий, а создание целостной образовательной среды, где современные ИКТ-инструменты делают процесс обучения интерактивным, адаптивным и ориентированным на индивидуальные потребности каждого студента [12].

Для реализации такой среды требуется сочетание нескольких взаимодополняющих мер:

– институциональные инициативы по поддержке и обеспечению равного доступа к цифровой инфраструктуре, особенно в регионах с ограниченными ресурсами;

– масштабная модернизация технической базы вузов и создание условий для полноценного онлайн-взаимодействия;

– системное развитие цифровой грамотности преподавателей и студентов с учётом психологических и социокультурных особенностей.

Успешное преодоление цифрового неравенства требует межсекторального сотрудничества между государством, бизнесом и образовательными учреждениями, а также разработки и внедрения нормативно-правовой базы в рамках развития информационного общества.

За последнее десятилетие в Республике Беларусь наблюдается значительный прогресс в преодолении цифрового неравенства благодаря развитию цифровой инфраструктуры и расширению доступа к высокоскоростному Интернету, особенно в сельских и удалённых регионах. По официальным данным Национального статистического комитета, удельный вес населения, использующего сеть Интернет, вырос к 2025 году до 94,3 % от общей численности [13]. Подписание Президентом Республики Беларусь *А.Г.Лукашенко* 1 апреля 2025 года Указа №139 «Об инвестиционном проекте», предусматривающего создание сети 5G, стало важным шагом на пути к дальнейшей цифровизации страны. Внедрение технологии 5G направлено на повышение доступности современных ИКТ-услуг, стимулирование экономического роста, привлечение инвестиций и укрепление технологического суверенитета.

На основе статистических данных о развитии ИКТ в учреждениях высшего образования Беларуси с 2016 по 2023 годы можно отметить положительную динамику в оснащении вузов компьютерной техникой и доступом к сети Интернет. За этот период общее количество персональных компьютеров, используемых в образовательном процессе, увеличилось с

29940 до 33870, а число компьютеров на 1000 студентов – с 170 до 218. Также наблюдается рост доли компьютеров, подключённых к сети Интернет, что свидетельствует о постепенном улучшении цифровой инфраструктуры в системе высшего образования страны [13]. Цифровая трансформация системы образования Республики Беларусь осуществляется в соответствие с Концепцией цифровой трансформации процессов в системе образования Республики Беларусь на 2019-2025 годы, утвержденной Министерством образования Республики Беларусь 15 марта 2019 года, которая представляет собой комплексный план модернизации образовательной сферы с использованием современных цифровых технологий. В её основе лежит модернизация инфраструктуры системы образования, направленная на обеспечение доступа к цифровым ресурсам и стабильную работу образовательных платформ. Особое внимание уделяется внедрению прорывных технологий, таких как искусственный интеллект, виртуальная и дополненная реальность, «умные учреждения» на базе интернета вещей, в том числе в формате «Smart School», что способствует повышению интерактивности и адаптивности учебного процесса. Одновременно происходит оптимизация и оцифровка всех процессов, протекающих в системе образования, с помощью программных средств, что повышает эффективность и прозрачность управления и обучения. Для реализации этих задач разрабатываются технические, программные, методические и нормативные решения, обеспечивающие безопасность данных и подготовку кадров. В результате данная концепция создаёт условия для формирования современной, технологически оснащённой и гибкой системы образования, способной эффективно адаптироваться к вызовам цифровой эпохи и обеспечивать высокое качество образовательных услуг.

Проблемы цифровой безопасности представляют собой следующий важный аспект устойчивого развития информационной экономики.

Современное информационное общество характеризуется высокой степенью зависимости от ИКТ, что, в свою очередь, обуславливает уязвимость как отдельных субъектов, так и целых государств перед лицом киберугроз. В научной и прикладной литературе под *информационной безопасностью* принято понимать совокупность мер, направленных на обеспечение конфиденциальности, целостности и доступности информации вне зависимости от формы её представления – цифровой или аналоговой. *Кибербезопасность,* в свою очередь, представляет собой более узкую категорию, фокусирующуюся исключительно на защите цифровых систем, сетей и данных от несанкционированного доступа, разрушения или модификации. Несмотря на различие в определениях, в условиях современной технологической конвергенции границы между этими понятиями становятся всё более размытыми, что требует комплексного и междисциплинарного подхода к формированию стратегий информационной защиты.

Одной из ключевых проблем в области информационной безопасности является усложнение характера угроз. Как отмечает специалист в сфере кибербезопасности *Н. Кшетри* современные кибератаки характеризуются высокой степенью целенаправленности, скрытности и технологической изощрённости. В частности, наблюдается рост числа инцидентов, связанных с применением программ-вымогателей, вредоносного программного обеспечения, атак на встроенные системы, а также методов социальной инженерии [14]. Эти угрозы требуют от специалистов не только глубоких технических знаний, но и способности к стратегическому мышлению, а также понимания поведенческих и организационных аспектов безопасности. По мнению *С. Каднаги* человеческий фактор продолжает оставаться одной из наиболее уязвимых составляющих информационной системы: ошибки пользователей, недостаточная осведомлённость персонала, несоблюдение протоколов

безопасности и использование слабых аутентификационных механизмов нередко становятся причиной серьёзных инцидентов [15].

В 2024 году мировой рынок услуг в области информационной безопасности существенно вырос, достигнув объема в 354,57 миллиардов долларов США, что на 21% больше показателей 2023 года. Зарубежные компании все активнее внедряют комплексные стратегии защиты, опираясь на современные технологии, такие как ИИ, машинное обучение и технологии-блокчейн, которые позволяют повысить эффективность обнаружения и предотвращения угроз. При этом злоумышленники также используют новые технологии для совершенствования кибер-атак.

Рост спроса на решения в сфере кибербезопасности поддерживается ужесточением нормативных требований по защите данных и расширением цифровой инфраструктуры, включая облачные сервисы и интернет вещей, что создает дополнительные уязвимости.

Лидирующими сегментами рынка остаются решения для защиты облачных ресурсов и данных, а также безопасность сетей и облачных сервисов. Географически наибольшие затраты несут правительственные и частные компании в Северной Америке, за ней следуют Европа и Азиатско-Тихоокеанский регион. Прогнозы аналитиков указывают на продолжение высокого темпа роста рынка с ожидаемым среднегодовым приростом около 21%, что к 2035 году может привести к увеличению глобальных расходов в сфере информационной безопасности до триллиона долларов США [16]. В Беларуси число киберпреступлений также продолжает расти: если в 2023 году они составляли около 21,5% от всех преступлений, то в первой половине 2024 года их доля увеличилась до 27,9%, превысив четверть от общего числа преступлений [17].

На международном уровне ситуация усугубляется отсутствием единых стандартов и согласованных правовых норм в области информационной безопасности. Различия в национальных

законодательствах, подходах к защите данных и терминологической базе затрудняют координацию усилий в борьбе с трансграничными угрозами. Это особенно актуально в условиях, когда киберпространство становится ареной геополитического противостояния, а кибератаки используются в качестве инструмента давления, шпионажа и дестабилизации.

Трансграничность данных процессов и открытость экономических субъектов делают национальную экономику более уязвимой к внешним угрозам, что создает риски информационно-технического воздействия со стороны зарубежных стран, направленного на подрыв информационной инфраструктуры в политических, экономических и военных целях. Кроме того, усиливается деятельность организаций, занимающихся технической разведкой в отношении государственных и коммерческих структур, что также требует повышенного внимания.

22 февраля 2023 года Высший Государственный Совет Союзного Государства России и Беларуси, утвердил Концепцию информационной безопасности. Этот документ подготовлен благодаря тесному сотрудничеству государственных органов двух стран и направлен на защиту их национальных интересов в информационной сфере. Концепция задаёт общие принципы и меры для обеспечения безопасности информационных систем, особенно критически важных объектов, а также противодействия вредоносному воздействию на информационные ресурсы Союзного государства. При этом обе страны действуют в международном информационном пространстве, учитывая международное право и национальные законы, чтобы поддерживать социальное и экономическое развитие, а также безопасность на региональном и глобальном уровнях. Реализация Концепции происходит совместно с партнёрами на международной площадке ООН. В частности, Беларусь и Россия участвуют в работе Специального комитета по созданию Конвенции

против преступного использования ИКТ и в Рабочей группе открытого состава по вопросам безопасности ИКТ в период с 2021 по 2025 годы [18].

В этом контексте особую роль играет политика цифрового протекционизма, проводимая рядом государств, в первую очередь США, которые под предлогом обеспечения национальной безопасности ограничивают доступ к технологиям, программному обеспечению и цифровым платформам для определённых стран. Подобные меры не только подрывают принципы свободного и равноправного цифрового взаимодействия, но и способствуют фрагментации глобального цифрового пространства, что, в свою очередь, увеличивает риски технологической изоляции, снижает совместимость систем и способствует росту уязвимостей.

Отдельного внимания заслуживает политика новой американской администрации в сфере высоких технологий. *Д.Трамп*, несмотря на традиционную для США осторожность в вопросах технологического регулирования, явно делает ставку на поддержку гигантов американской ИТ-индустрии. Одним из первых решений Трампа уже стало выделение миллиардов долларов США инвестиций на развитие ИИ в США, что свидетельствует о намерении сделать эту отрасль ключевым приоритетом американской экономической политики.

Новый курс *Д.Трампа* несет с собой как угрозы, так и возможности для белорусской экономики. Усиление санкционного давления, ограничение доступа к технологиям и торговая война США с ключевыми торговыми партнерами создают серьезные вызовы, которые потребуют от Беларуси пересмотра своих стратегий. Вместе с тем снижение цен на энергоносители и временное ослабление фокуса внимания ЕС на Восточной Европе могут предоставить Беларуси дополнительное время для адаптации к новым реалиям информационной экономики.

В ответ на эти вызовы в Беларуси утвердили Концепцию обеспечения суверенитета в сфере цифрового развития до 2030 года. Это предусмотрено постановлением Совета Министров от 31 декабря 2024 года №1074. В документе декларируется, что под суверенитетом в сфере цифрового развития понимается «неотъемлемое право государства управлять государственной информационно-коммуникационной инфраструктурой и информационными ресурсами, осуществлять над ними контроль, защищать свои интересы, проводить независимую внешнюю и внутреннюю государственную политикув сфере цифрового развития» [19]. Обеспечение суверенитета в этой области является частью обеспечения информационной безопасности Республики Беларусь.

Ключевые уязвимости цифрового суверенитета снижают доступ к международному программному и аппаратному обеспечению, что может привести к технологической изоляции. Использование иностранных облачных сервисов увеличивает риски утечек данных и потери контроля над стратегически важной информацией. Недостаток специалистов в ИТ-сфере и их релокация также сокращают потенциал цифровой трансформации. Монополизация ИТ-рынка иностранными поставщиками и отсутствие единого подхода к цифровой трансформации усложняют интеграцию систем государственного управления и снижают доверие граждан к электронным сервисам.

Одним из наиболее заметных последствий санкционного давления является ограничение доступа к зарубежным ИТ-решениям, что создает необходимость в активном процессе импортозамещения программного обеспечения, и, в свою очередь, требует комплексной перестройки существующих каналов передачи данных и технологий. В этих условиях важным аспектом является сотрудничество с Россией в рамках создания совместных импортозамещающих производств. Например, в России создан стратегический проект «Иннопрактика» – негосударственный институт

развития, реализующий стартапы, направленные на рост национального человеческого капитала, в том числе через структуры и механизмы информационной экономики. 6 марта 2025 года с участием данной ассоциации и представителей Парка высоких технологий при участии Постоянного комитета Союзного государства обсуждались направления синхронизации программ поддержки ИТ-компаний двух стран [20]. Это сотрудничество может стать ключевым фактором в преодолении технологической изоляции и обеспечении доступа к необходимым ресурсам информационного развития. Сотрудничество с Китаем также открывает новые перспективы для белорусской экономики. Растущая роль Китая как глобального технологического лидера предоставляет возможности для привлечения инвестиций и технологий, которые могут помочь Беларуси в модернизации экономики и развитии новых цифровых решений. Реализовать подобный потенциал сотрудничества мы предлагаем с помощью *системы информационных кластеров.*

В ближайшие годы Беларусь вступает в фазу активной реализации новой стратегии цифрового суверенитета. В условиях стремительного технологического прогресса страна стремится сочетать независимость в цифровой сфере с интеграцией в проекты Союзного государства России и Беларуси и ЕАЭС. Цифровая трансформация национальной экономики требует взвешенной политики, направленной на обеспечение национальной безопасности и устойчивого экономического развития. Поэтому Беларусь делает акцент на развитие собственных ИТ-ресурсов и укрепление цифровой устойчивости.

Тем не менее, эксперты подчеркивают, что все эти амбициозные планы могут остаться нереализованными, если не будет решена главная проблема – дефицит кадров и развитие сферы ИТ-образования. Даже с доступом к передовым технологиям и выходом белорусского ИТ-сектора

на мировой рынок, без квалифицированных кадров стране будет сложно реализовать свой потенциал в полной мере.

Таким образом, обеспечение информационной безопасности Республики Беларусь в условиях цифровой трансформации требует системного, междисциплинарного и проактивного подхода. Необходимо не только совершенствование технических средств защиты, но и развитие культуры информационной безопасности, повышение уровня цифровой грамотности населения, внедрение эффективных организационных и правовых механизмов, а также формирование устойчивых международных институтов сотрудничества с партнерами из России и ЕАЭС.

Использованные источники:

1. Understanding the Digital Divide // OECD Digital Economy Papers. – URL: https://www.oecd.org/content/dam/oecd /en/publications/reports/2001/01/understanding-the-digital-divide_g17a1b56/236405667766.pdf (дата обращения 12.12.2024)
2. Robinson L., Cotten S. R., Ono H., Quan-Haase A., Mesch G., Chen W., Stern M. J. Digital inequalities and why they matter // Information, Communication & Society. – 2015. – Vol. 18, № 5. – P. 569–582.
3. Van Dijk J.A. Digital divide research, achievements and shortcomings // Poetics. – 2006. – Vol. 34. – P. 221–235.
4. Статистика интернета и соцсетей на 2025 год – цифры и тренды в мире и в России // WebCanape. – URL: https://www.web-canape.ru/business/statistika-interneta-i-socsetej-na-2025-god-cifry-i-trendy-v-mire-i-v-rossii/?utm_referrer=https%3a%2f%2fwww.google.com%2f (дата обращения 12.12.2024)
5. Вартанова Е. Л., Гладкова А. А. Цифровое неравенство, цифровой капитал, цифровая включенность: динамика теоретических подходов и политических решений // Вестник Московского университета. Серия 10: Журналистика. – 2021. – № 1. – С. 3-29
6. Добринская Д. Е. Что такое цифровое общество? // Социология науки и технологий. – 2021. – Т. 12, № 2. – С. 112-129.
7. Бурдье П. Формы капитала // Экономическая социология. – 2002. – Т. 3. – № 5. – С. 60-74.
8. Granovetter M. S. The Strength of Weak Ties // The American Journal of Sociology. – 1973. – №78 (6). – P. 1360–1380

9. Flap H. No Man is an Island. The Research Program of a Social Capital Theory // Conventions and Structures in Economic Organization; ed. by O. Favereau, E. Lazega. – Northampton: Edward Elgar Publishing, Inc., 2002 . – 384 p. P.29-60.

10. Portes A. Economic Sociology and the Sociology of Immigration: a Conceptual Overview // The Economic Sociology of Immigration: Essays on Networks, Ethnicity, and Entrepreneurship. – N.Y.: Russell Sage Foundation, 1998. – 326 p.

11. Напсо М.Д. Цифровое неравенство и сфера образования // Человеческий капитал. – 2024. – № 2 (182). – С. 150-155

12. Баранов А.М., Лемещенко П.С. Образование как социальный институт: эволюция концепций и новые направления развития // Экономическое возрождение России. – 2022. – №3. – С.100-110.

13. Статистический сборник «Информационное общество в Республике Беларусь»; ред. колл. И.В. Медведева [и др.]– Минск, 2023. – 66 с.

14. Kshetri N. The Emerging Role of Big Data in Key Development Issues: Opportunities, Challenges, and Concerns // Big Data & Society. – 2014. – Vol. 1, No. 2. – P. 1–20.

15. Hadnagy C. Social Engineering: The Science of Human Hacking. – 2nd ed. – Hoboken, NJ: Wiley, 2018. – 320 p.

16. Информационная безопасность (мировой рынок) // TAdviser. – URL: https://www.tadviser.ru/index.php/Статья:Информационная _безопас ность_(мировой_рынок) (дата обращения: 01.04.2024).

17. Эксперты рассказали о количестве киберпреступлений в Беларуси // MyFin . – URL: https://myfin.by/article/biznes/eksperty-rasskazali-o-kolicestve-kiberprestuplenij-v-belarusi-33983 (дата обращения: 01.04.2024).

18. Об утверждении Концепции информационной безопасности Союзного государства // Министерство иностранных дел Республики Беларусь. – URL: https://mfa.gov.by/press/news_mfa/e0cd393f8e88ea17.html (дата обращения: 01.04.2024).

19. О Концепции обеспечения суверенитета Республики Беларусь в сфере цифрового развития до 2030 года // Национальный правовой Интернет-портал Республики Беларусь. – URL: https://pravo.by/document/?guid=125 51&p0=C22401074 (дата обращения: 01.04.2025).

20. В Минске в Парке высоких технологий прошла встреча с представителями российской компании «Иннопрактика» // Постоянный Комитет Союзного государства. – URL: https://посткомсг.рф/activities/events/241944/ (дата обращения: 01.04.2025).