УДК 004.056:330.101.5

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КАК ФАКТОР ЭКОНОМИЧЕСКОЙ СТАБИЛЬНОСТИ ГОСУДАРСТВА И БИЗНЕСА

А. Д. Волгина[1)], О. В. Миронович[2)], М. С. Щура[3)]

[1)] *студент, Белорусский государственный университет, г. Минск, Беларусь, alexandra.volgina7@gmail.com*
[2)] *студент, Белорусский государственный университет, г. Минск, Беларусь, mironovich986@gmail.com*
[3)] *студент, Белорусский государственный университет, г. Минск, Беларусь, maryshch18@gmail.com*

Научный руководитель **И. Н. Бородавка**

старший преподаватель, Белорусский государственный университет, г. Минск, Беларусь, Baradauka@bsu.by

В статье рассматриваются ключевые угрозы, связанные с утечками данных, вирусными атаками и вмешательством в критическую инфраструктуру. Приводятся примеры масштабных инцидентов, подтверждающих прямую связь между киберугрозами и экономическими последствиями для бизнеса и государства. Особое внимание уделяется международному опыту регулирования в области ИБ (ЕС, США), экономической целесообразности инвестиций в кибербезопасность. Сделан вывод о необходимости интеграции информационной безопасности в стратегическое планирование для обеспечения устойчивого экономического роста и доверия со стороны общества и инвесторов.

Ключевые слова: информационная безопасность, кибербезопасность, макроэкономическая стабильность, киберугрозы, цифровизация, утечка данных, киберпреступность.

INFORMATION SECURITY AS A FACTOR OF ECONOMIC STABILITY OF THE STATE AND BUSINESS

A. D. Volgina[1)], O. V. Mironovich[2)], M. S. Shchura[3)]

[1)] *student, Belarusian State University, Minsk, Belarus, alexandra.volgina7@gmail.com*
[2)] *student, Belarusian State University, Minsk, Belarus, mironovich986@gmail.com*
[3)] *student, Belarusian State University, Minsk, Belarus, maryshch18@gmail.com*

Supervisor **I. N. Borodavka**

senior lecturer, Belarusian State University, Minsk, Belarus, Baradauka@bsu.by

The article examines the key threats associated with data leaks, virus attacks, and interference in critical infrastructure. Examples of large-scale incidents are given, confirming a direct link between cyber threats and economic consequences for business and the state. Special attention is paid to the international experience of regulation in the field of information security (EU, USA), the economic feasibility of investments in cybersecurity. It is concluded that it is necessary to integrate information security into strategic planning to ensure sustainable economic growth and trust from society and investors.

Keywords: information security, cybersecurity, macroeconomic stability, cyber threats, digitalization, data breach, cybercrime.

В условиях цифровизации государственного управления и деятельности предприятий информационная и кибербезопасность становятся важнейшими элементами экономической устойчивости. Рост количества кибератак, утечек данных и дестабилизация цифровой инфраструктуры напрямую влияет на макроэкономические показатели: инвестиционную привлекательность, стабильность финансовых систем, доверие к институтам. Цель статьи – проанализировать влияние информационной безопасности на макроэкономическую стабильность и предложить рекомендации для государств и бизнеса.

Информационная безопасность (ИБ) – это защита важной информации от несанкционированного доступа, раскрытия, использования, изменения или нарушения работы.

Наибольшее количество кибератак терпит финансовый сектор. Сфера здравоохранения, а особенно медицинские базы данных также являются частой целью киберпреступников (28 %). В последнее время участились атаки на энергетическую инфраструктуру. По данным IBM Security, примерно 11 % всех кибератак по-прежнему приходится на сектор энергетики и коммунальных услуг [4]. Одна из крупнейших атак на коммунальные службы в 2024 году была совершена на нефтесервисный гигант Halliburton, который сообщил об убытках в размере $35 миллионов в результате кибератаки. Также под угрозой находится малый бизнес, не обладающий достаточными ресурсами для защиты (48 % всех атак). Внедрение комплексных систем управления информационными рисками способствует росту конкурентоспособности и устойчивости бизнеса.

Одними из наиболее серьёзных для государств и предприятий угроз ИБ являются утечки персональных и коммерческих данных и вмешательство в инфраструктуру критической значимости. Так произошла самая крупная утечка данных в Индии, где правительственная база данных Aadhaar, где хранятся идентификационные данные населения, подверглась многочисленным нарушениям, которые скомпрометировали записи 1,1 миллиарда зарегистрированных граждан.

Вирусные атаки также являются серьёзной угрозой. Компьютерные вирусы нарушают работу систем, вызывают серьезные сбои в работе и приводят к потере и утечке данных. В 2004 году Mydoom, ставший самой масштабной вспышкой компьютерного вируса в истории, нанес ущерб, по оценкам, в размере $38 миллиардов долларов, но с учетом инфляции на 2025 год составляет $52,2 миллиарда. Ещё один компьютерный вирус WannaCry в 2017 взломал компьютеры в 150 странах, что привело к значительному снижению производительности, поскольку предприятия, больницы и правительственные организации были вынуждены перестраивать системы с нуля [5].

Утечка информации напрямую влияет на экономическую стабильность. По данным IBM, средняя стоимость утечки данных в 2024 году составила более $4,88 млн [2]. Для малых и средних предприятий это огромные потери. Утечки также приводят к снижению инвестиционной привлекательности. Утечка данных клиентов или граждан снижает доверие населения и контрагентов. Исследование PWC показало, что 74 % потребителей заявили, что прекратили бы сотрудничество с компанией после утечки данных [6]. Также, утечки данных, саботаж или нестабильные ИТ-инфраструктуры могут отпугнуть инвесторов и снизить ВВП, вызвать панику, сбой в расчетах, отток капитала.

Государства и предприятия осознают необходимость развития информационной безопасности. Европейский акт о кибербезопасности (EU Cybersecurity Act) вводит общеевропейскую систему сертификации продуктов, услуг и процессов ИКТ в области кибербезопасности. Общие расходы предприятий по всему ЕС на внедрение правил кибербезопасности в рамках NIS2 оцениваются в $31,2 миллиарда в год [1]. Но, учитывая глобальные потери из-за киберпреступности, которые оцениваются в $5,5 трлн, эта цифра кажется маленькой.

По данным международной компании Howden, занимающейся киберстрахованием, компании, которые правильно инвестируют в кибербезопасность, получают рентабельность инвестиций в размере 25 %. Но, что более важно, они снижают затраты на кибератаки более чем на 75 % [3].

Информационная и кибербезопасность являются ключевыми условиями макроэкономической стабильности. Защита финансовой системы и критической инфраструктуры снижает риски сбоев, утечек и атак, обеспечивая непрерывность производственных и логистических процессов. Безопасная цифровая среда укрепляет доверие инвесторов и потребителей, снижает инфляционные ожидания и поддерживает стабильность. Защита интеллектуальной собственности и стратегических данных способствует технологическому лидерству и экономическому суверенитету.

Масштаб угроз подтверждает статистика: около 48 % атак приходится на малый бизнес, 28 % – на сферу здравоохранения, а 11 % – на энергетику и коммунальные услуги. Средняя стоимость утечки данных в 2024 году превысила $4,88 млн, а глобальные потери от киберпреступности оцениваются в $5,5 трлн ежегодно. В то же время инвестиции в киберзащиту способны снижать затраты на кибератаки более чем на 75 % и обеспечивать рентабельность вложений до 25 %.

Таким образом, кибербезопасность становится неотъемлемым фактором устойчивого экономического развития и глобальной конкурентоспособности.

Библиографические ссылки

1. Assessing the economic impact of eu initiatives on cybersecurity // frontier economics. URL: https://www.frontier-economics.com/media/izyk5rgz/assessing-the-economic-cost-of-eu-initiatives-on-cybersecurity.pdf – (дата обращения: 17.09.2025).

2. Cost of a data breach 2024: Financial industry // IBM. URL: https://www.ibm.com/think/insights/cost-of-a-data-breach- 2024-financial-industry (дата обращения: 17.09.2025).

3. *Gañán C. H., Ciere M., van Eeten M.* Beyond the pretty penny: the Economic Impact of Cybercrime // Proceedings of the 2017 New Security Paradigms Workshop (NSPW '17). New York : Association for Computing Machinery, 2017. C. 35–45. URL: https://doi.org/10.1145/3171533.3171535 (дата обращения: 19.09.2025).

4. IBM X-Force 2025 Threat Intelligence Index // IBM. URL: https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/2025-threat-intelligence-index (дата обращения: 19.09.2025).

5. *Joshi M. J., Patil B. V.* Computer Virus: Their Problems & Major Attacks in Real Life // International Journal of P2P Network Trends and Technology (IJPTT). 2013. Vol. 3, issue 4. P. 206. URL: http://www.ijpttjournal.org (дата обращения: 19.09.2025).

6. Survey: 59 % of US companies would have 2 weeks of stock after halting production // SupplyChainDive. URL: https://www.supplychaindive.com/news/coronavirus-survey-us-companies-shipments-after-production-stops/575026/ (дата обращения: 20.09.2025).