УДК 004.056:330.131.7
DOI 10.26118/2782-4586.2025.16.58.043

Байбеков Алан Тимурович
Кубанский Государственный Технологический Университет
Лесникова Наталья Евгеньевна
Кубанский Государственный Технологический Университет

Экономическое моделирование последствий масштабных кибератак на критическую инфраструктуру: оценка системного риска для национальной экономики

Аннотация. Актуальность исследования обусловлена растущей угрозой масштабных кибератак для объектов критической инфраструктуры в условиях цифровой трансформации экономики. Проблема заключается в отсутствии комплексных методик, позволяющих оценивать не только прямые, но и системные макроэкономические последствия таких инцидентов. Целью работы является разработка модели для количественной оценки системного риска на основе модифицированной модели «затраты-выпуск». Методология позволяет учесть каскадный эффект и косвенные потери в смежных отраслях вследствие нарушения межотраслевых связей. Результаты сценарного моделирования атаки на энергетический сектор демонстрируют, что совокупные потери для национальной экономики могут многократно превосходить прямой ущерб, достигая 2.5% ВВП и более. Полученные выводы подчеркивают необходимость учета системных рисков органами государственного управления при разработке стратегий киберустойчивости.

Ключевые слова: кибератаки, критическая инфраструктура, экономическое моделирование, системный риск, макроэкономические последствия, модель «затраты-выпуск»

Baibekov Alan Timurovich
Kuban State Technological University
Lesnikova Natalia Evgenievna
Kuban State Technological University

Economic modeling of large-scale cyberattacks on critical infrastructure: assessment of systemic risk for the national economy

Annotation. The relevance of the study is driven by the growing threat of large-scale cyberattacks on critical infrastructure amid the digital transformation of the economy. The problem lies in the lack of comprehensive methodologies to assess not only direct but also systemic macroeconomic consequences of such incidents. The aim is to develop a model for the quantitative assessment of systemic risk based on a modified input-output model. The methodology accounts for cascade effects and indirect losses in interrelated industries due to disruptions in inter-industry linkages. The results of scenario modeling of an attack on the energy sector demonstrate that total losses for the national economy can far exceed direct damage, reaching 2.5% of GDP or more. The findings highlight the need for government authorities to consider systemic risks when developing cyber resilience strategies.

Keywords: cyberattacks, critical infrastructure, economic modeling, systemic risk, macroeconomic consequences, input-output model.

Введение

Растущая зависимость критической инфраструктуры (КИ) - энергетики, финансов, транспорта, здравоохранения - от цифровых технологий создает беспрецедентные

уязвимости для национальной экономики. По оценкам Банка международных расчетов, потенциальные потери от кибератак на финансовую систему могут достигать 5% ВВП, а в некоторых развивающихся странах - превышать 10% ВВП. Исследование, проведенное в России, показало, что ущерб от успешных кибератак может достигать 2.7% ВВП, что эквивалентно 5.3 трлн рублей. Глобальный анализ Lloyd's указывает на возможность колоссальных потерь в размере до $3.5 трлн для мировой экономики в случае атаки на ключевую платежную систему.

Особенностью современных киберугроз является их трансграничный и каскадный характер, когда инцидент в одном секторе быстро распространяется на другие, связанные с ним через межотраслевые цепочки поставок и производственные связи. Несмотря на это, существующие подходы к оценке ущерба часто фокусируются на прямых, локализованных потерях для атакованной организации, игнорируя системные эффекты.

Целью данного исследования является разработка модели для количественной оценки системного риска для национальной экономики от масштабных кибератак на критическую инфраструктуру. Для достижения цели решаются следующие задачи: анализ каналов трансмиссии кибершоков; адаптация метода экономического моделирования «затраты-выпуск» для учета кибер-инцидентов; сценарное моделирование атаки на ключевой сектор и оценка совокупных потерь ВВП.

Результаты исследования

В качестве методологической основы исследования выбрана модифицированная модель «затраты-выпуск» В. Леонтьева. Данный подход позволяет количественно оценить как прямые потери сектора, подвергшегося атаке (снижение выпуска), так и косвенные потери в смежных отраслях, возникающие из-за нарушения межотраслевых поставок. Модель эффективно описывает каскадные эффекты (cascading failures), являющиеся следствием взаимозависимости секторов экономики.

Для проведения расчетов использовались данные условной межотраслевой балансовой таблицы, агрегированные в семь ключевых секторов: Энергетика, Финансовые услуги, Обрабатывающая промышленность, Транспорт, Сельское хозяйство, IT и связь, Прочие услуги. Были построены три сценария кибератаки на энергетический сектор, различающиеся по длительности и интенсивности воздействия:

1. Сценарий 1 (легкий): Кратковременная атака, приводящая к снижению выпуска энергетического сектора на 10% в течение одного расчетного периода.
2. Сценарий 2 (умеренный): Атака средней продолжительности, вызывающая снижение выпуска на 25%.
3. Сценарий 3 (тяжелый): Затяжная и высокоинтенсивная атака, приводящая к снижению выпуска на 40%.

Таблица 1. Расчет прямых и косвенных потерь выпуска по секторам экономики (%)

Сектор экономики	Сценарий 1	Сценарий 2	Сценарий 3
Энергетика	-10.0	-25.0	-40.0
Обрабатывающая промышленность	-3.2	-8.1	-13.2
Транспорт	-2.1	-5.4	-8.9
Финансовые услуги	-1.5	-3.8	-6.3
Сельское хозяйство	-1.8	-4.6	-7.6
Совокупные потери ВВП	-0.5%	-1.3%	-2.5%

Результаты моделирования, представленные в Таблице 1, наглядно демонстрируют значительный мультипликативный эффект. Прямое воздействие на энергетику вызывает существенные косвенные потери в промышленности, транспорте и других секторах, которые зависят от энергопоставок. В тяжелом сценарии совокупные потери ВВП достигают 2.5%, что более чем в 6 раз превышает прямой спад в энергетике в относительном выражении. Это подтверждает гипотезу о доминировании косвенных потерь в общей структуре ущерба.

Наиболее уязвимыми к шоку в энергетике оказываются сектора с высокой зависимостью от непрерывного энергоснабжения и жесткими технологическими цепочками - обрабатывающая промышленность и транспорт. Финансовый сектор, несмотря на относительно высокую зрелость киберзащиты, также несет значительные косвенные убытки из-за нарушения операционной деятельности и падения потребительской активности.

Выводы

Проведенное исследование подтвердило, что системные макроэкономические последствия масштабных кибератак на критическую инфраструктуру многократно превосходят прямой ущерб, нанесенный атакованному сектору. Разработанная на основе модели «затраты-выпуск» методика позволяет количественно оценить каскадные эффекты и косвенные потери, возникающие в результате нарушения межотраслевых связей.

Полученные результаты имеют практическую значимость для органов государственного управления и регуляторов. Предложенная модель может быть использована для стресс-тестирования экономики, определения приоритетных направлений для инвестиций в кибербезопасность критической инфраструктуры и формирования стратегических резервов для смягчения макроэкономических последствий кибер-инцидентов.

Перспективы дальнейших исследований связаны с усовершенствованием модели за счет интеграции поведенческих факторов (таких как паника на рынках и изменение потребительского доверия), а также с разработкой комплексных моделей передачи киберриска, включающих инструменты страхования. Отдельную важность представляет сбор и стандартизация эмпирических данных о фактических потерях от кибератак для калибровки и верификации теоретических моделей.

Список источников

1. Центральные банки и риски кибербезопасности // ECONS.ONLINE. – 2022. – 19 октября. – URL: https://econs.online/articles/techno/tsentralnye-banki-i-riski-kiberbezopasnosti/
2. CODE RED 2026: Актуальные киберугрозы для российских организаций // Positive Technologies. – 2025. – URL: https://ptsecurity.com/research/analytics/russia-cyberthreat-landscape-2026/
3. Потери от киберпреступности // Tadviser. – 2025. – URL: https://www.tadviser.ru/index.php/Статья:Потери_от_киберпреступности
4. Counting the economic cost: How vulnerable could you be? // Lloyd's. – URL: https://www.lloyds.com/insights/futureset/futureset-insights/systemic-risk-scenarios/illuminating-cyber-crime/economic-impact
5. Оценка и управление рисками: как работает модель угроз информационной безопасности // Инфарс. – URL: https://infars.ru/blog/otsenka-i-upravlenie-riskami-kak-rabotaet-model-ugroz-informatsionnoy-bezopasnosti/
6. Методы моделирования атак // PT Research. – URL: https://ptresearch.media/articles/metody-modelirovaniya-atak
7. Российский бизнес провалил кибериспытания: 2,7% ВВП под угрозой // Компьютерра. – 2025. – URL: https://www.computerra.ru/320736/rossijskij-biznes-provalil-kiberispytaniya-2-7-vvp-pod-ugrozoj/
8. Systemic Cyber Risk and Aggregate Impacts // Risk Analysis. – 2022. – Vol. 42, Iss. 8. – P. 1606-1622. – DOI: 10.1111/risa.13715.

9. Оценка актуальных угроз ИБ // ESA PRO. – 2025. – 23 июля. – URL: https://esapro.ru/blog/otsenka-aktualnykh-ugroz-informatsionnoy-bezopasnosti/

10. RCVaR: An economic approach to estimate cyberattacks costs using data from industry reports // Computers & Security. – 2024. – Vol. 139. – DOI: 10.1016/j.cose.2024.103737.

Сведения об авторах

Байбеков Алан Тимурович, студент, ФГБОУ ВО «Кубанский Государственный Технологический Университет», г. Краснодар, Россия

Лесникова Наталья Евгеньевна, кандидат экономических наук, доцент, ФГБОУ ВО «Кубанский Государственный Технологический Университет», г. Краснодар, Россия

Information about the authors

Baibekov Alan Timurovich, student, Kuban State Technological University, Krasnodar, Russia

Lesnikova Natalia Evgenievna, PhD in Economics, Associate Professor, Kuban State Technological University, Krasnodar, Russia