http://dx.doi.org/10.35596/1729-7648-2026-32-2-22-27

УДК 656.078.5:004

ПРИМЕНЕНИЕ ЭКОНОМИКО-МАТЕМАТИЧЕСКОГО ИНСТРУМЕНТАРИЯ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЪЕКТОВ ЛОГИСТИЧЕСКОЙ ИНФРАСТРУКТУРЫ

С. Ф. КУГАН, А. М. ВОРОНИНА

Белорусский государственный университет информатики и радиоэлектроники (Минск, Республика Беларусь)

Аннотация. Проведено исследование применяемых на объектах логистической инфраструктуры цифровых технологий. Сделан акцент на специфику логистической деятельности, цифровизация которой порождает новый класс угроз – киберфизических рисков, при реализации которых, помимо сбоев, в материальных потоках формируются мультипликативные экономические потери по всей цепи поставок. Рассмотрены экономико-математические модели, обоснована эффективность их применения для объектов логистической инфраструктуры. Доказана важность интегрированного подхода к управлению информационной безопасностью в условиях быстро меняющегося внешнего окружения.

Ключевые слова: киберинцидент, киберфизические риски, объекты логистической инфраструктуры, управление, экономико-математические модели.

Конфликт интересов. Авторы заявляют об отсутствии конфликта интересов.

Для цитирования. Куган, С. Ф. Применение экономико-математического инструментария в сфере информационной безопасности объектов логистической инфраструктуры / С. Ф. Куган, А. М. Воронина // Цифровая трансформация. 2026. Т. 32, № 2. С. 22–27. http://dx.doi.org/10.35596/1729-7648-2026-32-2-22-27.

APPLICATION OF ECONOMIC AND MATHEMATICAL TOOLS IN THE FIELD OF INFORMATION SECURITY OF LOGISTICS INFRASTRUCTURE FACILITIES

SVETLANA KUHAN, ALINA VORONINA

Belarusian State University of Informatics and Radioelectronics (Minsk, Republic of Belarus)

Abstract. This paper examines digital technologies used in logistics infrastructure facilities. It emphasizes the specific nature of logistics activities, whose digitalization creates a new class of threat – cyber-physical risks. These risks, when realized, not only disrupt material flows, but also cause multiplicative economic losses throughout the supply chain. Economic and mathematical models are examined, and their effectiveness for logistics infrastructure facilities is substantiated. The importance of an integrated approach to information security management in a rapidly changing external environment is demonstrated.

Keywords: cyber incident, cyber-physical risks, logistics infrastructure facilities, management, economic and mathematical models.

Conflict of interests. The authors declare that there is no conflict of interests.

For citation. Kuhan S., Voronina A. (2026) Application of Economic and Mathematical Tools in the Field of Information Security of Logistics Infrastructure Facilities. *Digital Transformation.* 32 (2), 22–27. http://dx.doi.org/10.35596/1729-7648-2026-32-2-22-27 (in Russian).

Введение

Современные тенденции в сфере логистики, призванные решать сложные творческие задачи, направлены в первую очередь на решение недетерминированных задач в режиме реального времени, а во вторую – на создание нового формата взаимодействия в системе «человек – машина», где человек рассматривается уже не как помеха, а как ценный ресурс, способный решать нетипичные задачи, контролируя при этом выполнение машинами стандартных, рутинных работ. Существующий спрос на эффективные логистические решения (рис. 1) обусловлен лавинным спросом на онлайн-покупки.

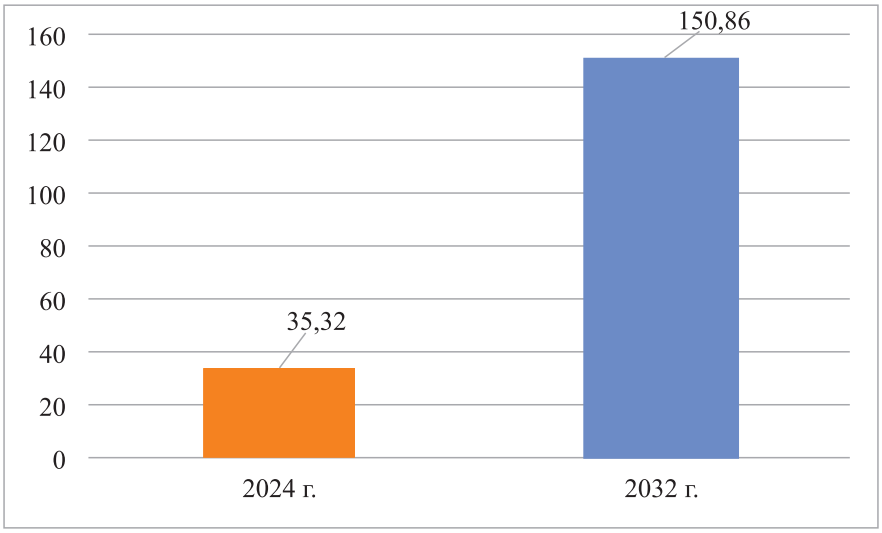

Рис. 1. Размер рынка логистических услуг [1]
Fig. 1. Logistics services market size [1]

Возрастающая требовательность со стороны покупателя вынуждает компании, в том числе и логистические, активно использовать цифровые логистические решения, снижая затраты за счет оптимизации складских операций, интеграции передовых технологий, прозрачности услуг доставки. Интеграция таких технологий, как интернет вещей (IoT), искусственный интеллект, машинное обучение и других, обеспечивает точность и оперативность принятия управленческих решений в режиме реального времени.

Однако при всех плюсах цифровизации оптимизм бизнеса несколько снизился из-за значительных первоначальных затрат, с которыми вынуждены считаться логистические компании и которые связаны с инвестициями в цифровые технологии, с обучением персонала, модернизацией устаревших систем, поддержанием работоспособности новой инфраструктуры и с экономическим ущербом от киберинцидентов. Современные технологии, помимо высоких капиталовложений, провоцируют материализацию специфических нефинансовых рисков, бьющих по операционной стабильности, подтверждая тот факт, что объекты логистической инфраструктуры критически зависимы от целостности цифрового контура, стабильности сигнала, отсутствия ошибок в коде и других нюансов.

Формулирование проблемного поля

Новой управленческой реальностью становится ситуация, когда деятельность объекта логистической инфраструктуры напрямую зависит от бесперебойной работы его IT-систем, а также от множественности векторов несанкционированных вторжений. И если в случаях физической поломки оборудования все ясно и понятно (замена изношенных деталей или покупка нового оборудования), то несанкционированное вторжение порождает мультипликативные эффекты за счет подключения смежных звеньев цепочки поставок. То есть имеет место нелинейная взаимосвязь между фактом несанкционированного вторжения (технологическим инцидентом) и последствиями (материальным (экономическим) ущербом).

Другими словами, речь идет об анализе критических точек входа, последствий вариантов несанкционированного доступа через каждую из них, о расчете финансовых последствий

выхода из строя всей или части логистической системы. В этих условиях возникает потребность в подборе экономико-математического инструментария, с помощью которого можно не только просчитать вероятность наступления рисковой ситуации, но и смоделировать каскадные последствия материализации киберинцидента, расчет которых невозможен простой калькуляцией потерь. Под киберинцидентом (цифровым инцидентом) понимается событие или последовательность событий в информационно-телекоммуникационной среде, повлекшее негативные последствия в виде нарушения функционирования системы или сети, целостности, доступности или конфиденциальности данных, а также в нанесении реального или потенциального ущерба охраняемым законом общественным отношениям.

Последствия от материализации киберугроз для объектов логистической инфраструктуры сложно рассчитать через стандартное нормальное распределение ущерба, так как в логистике имеет место каскадный операционный ущерб. Поэтому используемые в анализе модели должны содержать не только технологический (архитектура системы (SCADA, WMS, TMS, IoT-датчики)), но и экономический слой – поток создания стоимости (Just-in-Time, оборачиваемость запасов, штрафы за срыв соглашения по уровню обслуживания (SLA)). Данный синтез возможен через методологию киберфизических систем (CPS), объединяющую кибернетику и управление процессами. CPS представляет собой интеграцию вычислительных ресурсов в физические объекты с последующей возможностью прогнозирования, самонастройки и адаптации к изменениям. В CPS оборудование, включая цифровые датчики, и информационные системы работают как единый механизм на протяжении всей цепочки создания стоимости. По сути, CPS является основой для реализации сценариев развития производства посредством взаимодействия между физическими и цифровыми элементами системы.

Методика исследования

Имитационное моделирование, как наиболее эффективный инструмент анализа рисков, активно используется во всех сферах человеческой деятельности. Актуальность применения и распространенность систем имитационного моделирования рассмотрены в [2–4]. Так, в [4, с. 35] отмечается, что при выборе систем моделирования принято выделять системы проблемно-ориентированного (специализированные) и общецелевого назначения (универсальные). Специализированные имеют узкие области применения, например, OPNET (SteelCentral), COMNET (вычислительные сети), eMPlant, DELMIA (машиностроение и судостроение), ISSOP (производство и логистика), PTV Vision Vissim (транспортные потоки и дорожное движение). Для построения моделей в таких системах применяются готовые наборы типовых элементов моделируемого объекта.

Использование агентного и дискретно-событийного моделирования (ABM/DES) позволяет моделировать цифровой двойник системы (склад, транспортный узел) не непрерывно, а событийно. Данный подход дает возможность рассматривать каждый погрузчик, конвейер, строку в WMS как агента или событие. Моделирование сбоя, например ситуации отказа сервера или нарушения целостности данных в системе управления перевозками (TMS), позволяет рассматривать поведение агентов в конкретном временном интервале, исследовать каскадное распространение последствий в рамках всей цепочки поставок.

Провести оценку системных эффектов на уровне цепей поставок можно с помощью модели «затраты–выпуск» (межотраслевого баланса) Леонтьева с шоковыми переменными и деревьями событий (I/O Models с Event Trees). В основе данной модели лежит понимание взаимосвязанности процессов в экономике, т. е. сбой в одном элементе системы (временная остановка влечет за собой невозможность оказания услуги в полном объеме) через коэффициенты прямых затрат передается всем, кто от него зависит. При этом введение одной шоковой переменной недостаточно, необходимо проследить всю цепочку каскадных изменений, что возможно через дерево событий, переводящее технические сценарии в экономические величины – ожидаемый системный ущерб. По сути, реализуется связка, объединяющая матрицу прямых затрат, рисковое событие и последствия в итоговый мультипликационный эффект, представляющий собой сумму эффектов – прямого и косвенных (первого и второго порядков).

При выборе модели, позволяющей оценить последствия кибератак, стоит обратить внимание на модели гибридных сетей Петри, дающие возможность зафиксировать не только сам факт

несанкционированного входа, но и измерить его последствия – рассчитать объем недопоставленного ресурса как функцию от продолжительности блокировки управляющего сигнала и интенсивности потока. Эта возможность исходит из представления логистического объекта как двуслойной сети, в которой непрерывные маркеры (первый слой) – физические процессы, дискретные маркеры (второй слой) – информационные процессы. Смысл гибридных сетей Петри в том, что они в рамках одной математической схемы (графа, сети) связывают непрерывную динамику физического процесса с дискретностью цифровых управляющих команд.

Экономическая деятельность часто реализуется в условиях полной или частичной неопределенности, что повышает ее риски и не позволяет с полной уверенностью говорить о конечном результате. В данных условиях целесообразно использование модели «Байесовская сеть доверия», которая представляет собой направленный граф, выстраивающий причинно-следственные связи в условиях частичного отсутствия данных, и позволяет связать факты технологической уязвимости (архитектуру IT, квалификацию персонала и др.) с вероятностью киберугрозы, а также определить экономические последствия данной ситуации в рамках теории вероятности. Привлекательность такой модели заключается в возможности построения вероятностной модели и вычислении интегрального показателя киберуязвимости объекта, а также реализации обратного анализа, т. е. фактическая ситуация изучается сетью с раскладом до вероятностной первопричины цифровой природы, что позволяет разделять технологические и организационные риски.

Результаты исследований и их обсуждение

Исследование работ, посвященных информационной безопасности объектов критической инфраструктуры [5–7], к которой полноправно относятся объекты логистики, позволяет сделать вывод, что кибератака (киберинцидент) – это не только технический сбой, а целая система каскадных, нарастающих снежным комом проблем с огромными экономическими потерями: от остановок в звеньях цепей поставок до дефицита пропускной способности, потери координации и срыва поставок. Если говорить о различиях в природе киберинцидента и технического отказа оборудования, то главное отличие будет в векторе воздействия.

В случае технического отказа имеет место остановка функционирования оборудования. Как правило, он носит случайный, несистемный характер, в большинстве случаев локализован в пределах конкретной системы или компонента, а основная задача реагирования – восстановление штатной работоспособности инфраструктуры (например, появление на магнитном диске поврежденных участков, из-за чего часть файлов становится недоступна). Кибератака вызывает не только фактическую остановку, но и утрату контроля над процессом, снижение результативности управления, искажение истинной ситуации (например, атака на цепочку поставок, когда искажение данных в одном звене цепи может привести к ошибкам в планировании, перерасходу ресурсов, задержкам и проч.). Подобная ситуация формирует эмерджентный ущерб, когда экономические последствия представляют собой нелинейную реакцию всей логистической системы на утрату доверия к данным:

– один инцидент затрагивает множество организаций;

– лавинообразный эффект распространения;

– восстановление предполагает четкую координацию действий всех участников цепи.

В отличие от технического отказа киберинцидент носит целенаправленный характер: несанкционированный доступ к данным компании, намеренное их искажение, использование взаимосвязи между компонентами и организациями для расширения масштаба атаки. В случае материализации данного события собираются доказательства внешнего воздействия: подозрительные сетевые соединения, следы вредоносного программного обеспечения, несанкционированные изменения системных файлов или конфигураций, которые невозможно объяснить случайными сбоями. Важно исключить технические причины (экспертиза оборудования и программного обеспечения, отсутствие физических повреждений и проч.). Нелинейность реакции системы проявляется в том, что последствия несоразмерны первоначальному воздействию и возникают из-за каскадного распространения по сложным взаимосвязям (например, нарушение бизнес-процессов логистической сети). Остановка поставок одной компании вызывает задержки, штрафы или дополнительные затраты у ее партнеров, что фиксируется через анализ контрактов, журналы событий, финансовые отчеты и официальные обращения. Стандартное распределение

ущерба (нормальное, экспоненциальное) здесь неприменимо, так как в подобной ситуации отсутствуют стационарность и независимость событий. Для кибератаки свойственны асимметричные последствия, зависящие от динамики угроз и сетевых эффектов.

Заключение

1. Имитационное моделирование представляется целесообразным сочетать с моделью «затраты–выпуск», дополненной шоковыми переменными и деревьями событий, а также с гибридными сетями Петри и байесовскими сетями доверия. Это позволит связать технологический слой (SCADA, WMS, TMS, IoT) с экономическим и количественно оценить каскадный эффект киберинцидента.

2. Киберинцидент, в отличие от технического отказа, порождает потерю контроля и искажение данных, что вызывает нелинейный эмерджентный ущерб, мультиплицируемый по цепи поставок. Стандартные распределения ущерба здесь неприменимы.

3. Рекомендованы интегрированный подход на базе киберфизических систем и обратный анализ по байесовской сети для разделения технологических и организационных рисков.

4. Перспективы дальнейших исследований заключаются в создании типовых цифровых двойников для складов, хабов и портов, в совершенствовании моделей мультипликативных потерь с учетом санкций по SLA, интеграции с системами мониторинга информационной безопасности и углубленного анализа человеческого фактора в новой парадигме взаимодействия «человек – машина».

Список литературы

1. Анализ размера, доли и тенденций мирового рынка цифровой логистики – обзор отрасли и прогноз до 2032 года [Электронный ресурс]. Режим доступа: https://www.databridgemarketresearch.com/ru/reports/global-digital-logistics-market. Дата доступа: 09.04.2026.
2. Антюшеня, Д. М. Транспортно-логистическая система Республики Беларусь: становление и развитие / Д. М. Антюшеня. Минск: Белор. нац. техн. ун-т, 2016.
3. AnyLogic моделирование для обоснованных решений [Электронный ресурс]. Режим доступа: https://www.anylogic.ru/. Дата доступа: 25.04.2026.
4. Даденков, С. А. Анализ моделей и методов агентного и дискретно-событийного имитационного моделирования / С. А. Даденков, Е. Л. Кон // Известия СПбГЭТУ «ЛЭТИ». 2015. № 5. С. 35–41.
5. Реализация требований обеспечения безопасности критической информационной инфраструктуры с помощью автоматизации [Электронный ресурс]. Режим доступа: https://habr.com/ru/companies/securityvison/articles/1026904/. Дата доступа: 23.04.2026.
6. Биктубаева, К. С. К вопросу об обеспечении информационной безопасности объектов критической информационной инфраструктуры / К. С. Биктубаева // Информационные технологии обеспечения комплексной безопасности в цифровом обществе: материалы VII Всерос. молодеж. науч.-практ. конф. с междунар. участием, Уфа, 23–24 мая 2025 г. Уфа: Уфимский университет науки и технологий, 2025. С. 226–229.
7. Исмагилова, А. С. Теоретико-графовая интерпретация системы защиты информации / А. С. Исмагилова, И. А. Шагапов, И. В. Салов // Инженерный вестник Дона. 2024. № 9. С. 171–179.

Поступила 30.04.2026 Принята в печать 22.05.2026 Доступна на сайте 10.07.2026

References

1. *Analysis of the Size, Share, and Trends of the Global Digital Logistics Market – Industry Overview and Forecast to 2032*. Available: https://www.databridgemarketresearch.com/ru/reports/global-digital-logistics-market (Accessed 9 April 2026) (in Russian).
2. Antyushenya D. M. (2016) *Transport and Logistics System of the Republic of Belarus: Formation and Development*. Minsk, Belarusian National Technical University (in Russian).
3. *AnyLogic Modeling for Informed Decisions*. Available: https://www.anylogic.ru/ (Accessed 25 April 2026) (in Russian).
4. Dadenkov S. A., Kon E. L. (2015) Comparison of Agent-Based and Discrete-Event Simulation Models and Methods. *Bulletin of ETU "LETI"*. (5), 35–41 (in Russian).
5. *Implementation of Critical Information Infrastructure Security Requirements Using Automation*. Available: https://habr.com/ru/companies/securityvison/articles/1026904/ (Accessed 23 April 2026) (in Russian).

6. Biktubaeva K. S. (2025) On the Issue of Ensuring Information Security of Critical Information Infrastructure Facilities. *Information Technologies for Ensuring Comprehensive Security in a Digital Society, Proceedings of the VII All-Russian Youth Scientific and Practical Conference with International Participation, Ufa, May 23–24.* Ufa, Ufa University of Science and Technology. 226–229 (in Russian).
7. Ismagilova A. S., Shagapov I. A., Salov I. V. (2024) Graph-Theoretical Interpretation of the Information Security System. *Engineering Bulletin of the Don*. (9), 171–179 (in Russian).

Received: 30 April 2026 Accepted: 22 May 2026 Available on the website: 10 July 2026

Вклад авторов / Authors' contribution

Авторы внесли равный вклад в написание статьи / The authors contributed equally to the writing of the article.

Сведения об авторах

Куган С. Ф., д-р экон. наук, доц., нач. упр. подготовки научных кадров высшей квалификации, Белорусский государственный университет информатики и радиоэлектроники

Воронина А. М., магистр, асп. каф. экономики, Белорусский государственный университет информатики и радиоэлектроники

Адрес для корреспонденции

220013, Республика Беларусь,
Минск, ул. П. Бровки, 6
Белорусский государственный университет
информатики и радиоэлектроники
Тел.: +375 29 792-52-12
E-mail: sfkugan@mail.ru
Куган Светлана Федоровна

Information about the authors

Kuhan S., Dr. Sci. (Econ.), Associate Professor, Head of the Department for Training of Highly Qualified Scientific Personnel, Belarusian State University of Informatics and Radioelectronics

Voronina A., M. Sci., Postgraduate of the Department of Economics, Belarusian State University of Informatics and Radioelectronics

Address for correspondence

220013, Republic of Belarus,
Minsk, P. Brovki St., 6
Belarusian State University
of Informatics and Radioelectronics
Tel.: +375 29 792-52-12
E-mail: sfkugan@mail.ru
Kuhan Svetlana