

# КАТЕГОРНЫЙ ПОДХОД К ОЦЕНКЕ УЯЗВИМОСТИ КИБЕРФИЗИЧЕСКИХ СИСТЕМ

Волкова Е.С., Гисин В.Б.

Финансовый университет при Правительстве Российской Федерации, Россия, 125167, Москва, пр-кт Ленинградский, д. 49/2, тел. +7(916)253-27-26, E-mail: vgisin@fa.ru

Кибербезопасность в киберфизическом мире, является предметом многочисленных исследований, в которых применяется разнообразный математический аппарат и инструментарий современной информатики. С учетом этого актуальным является вопрос систематизации используемых методов и выработки общих концепций, которые могли бы служить платформой для таких исследований [1]. В настоящей работе представлен формальный метод описания действий злоумышленника на уровне компонентов системной модели. Киберфизическая система рассматривается как объект категории систем над моноидальной категорией [2]. Формализм теории категорий является адекватным инструментом для описания декомпозиции систем, введения понятия угрозы на уровне модельного строения системы. В [3] алгебраический формализм теории категорий использовался для анализа угроз с использованием леммы Йонеды.

В настоящей работе развит более общий подход, при котором системы рассматриваются в категории линз с монадой, моделирующей неопределенность. При таком подходе неопределенность может быть представлена как распределениями вероятности в пространстве состояний, так и логическими оценками состояний. Использование аппарата теории категорий позволяет с единой точки зрения рассматривать дискретные модели и непрерывные модели (представленные системами дифференциальных уравнений, в том числе и нелинейных), композицию и взаимодействие таких разнородных систем.

## Литература.

1. *Trenchev I., Dimitrov W., Dimitrov G., Ostrovska T., Trencheva M.* Mathematical approaches transform cybersecurity from protoscience to science // *Applied Sciences* 13, 11, 2023, p. 6508. <https://doi.org/10.3390/app13116508>
2. *Vidalie J., Batteux M., Mhenni F., Choley J. Y.* Category theory framework for system engineering and safety assessment model synchronization methodologies // *Applied Sciences* 12, 12, 2022, p. 5880. <https://doi.org/10.3390/app12125880>
3. *Bakirtzis G., Genovese F., Fleming C. H.* Yoneda hacking: The algebra of attacker actions // *ACM Transactions on Cyber-Physical Systems (TCPS)* 6, 3, 2022, p. 1-27. <https://doi.org/10.1145/3531063>