

**Рецензия на статью Попова В.Ю.
«О скрытых структурах булевых функций»**

Статья посвящена изучению вычислительной сложности нахождения правильных значений переменных скрытых структур булевых функций. Определение скрытых структур булевых функций облегчает решение различных вычислительно трудных алгоритмических проблем, например, проблемой выполнимости булевых формул. В задачах, связанных с криптографией, известно, что решение есть, а проблема состоит в поиске правильных значений соответствующих переменных. В работе рассматриваются сильно связанные компоненты булевых функций, которые могут быть найдены за полиномиальное время. Автор доказывает, что проблема нахождения правильных значений переменных сильно связанных компонент является вычислительно трудной. Особый интерес, по мнению рецензента, представляет Предложение 4 о том, что множество всех полиномиальных недетерминированных машин Тьюринга, решающих проблемы из класса **TFNP**, не является рекурсивно перечислимым. Это является серьезным аргументом в пользу того, что в классе **TFNP** нет полных проблем.

Полученные результаты являются, по мнению рецензента, достаточно интересными для специалистов по теории сложности вычислений, в частности для исследований проблемы выполнимости и для криптографических приложений. Доказательства теорем полные и хорошо обоснованные. Статья также содержит исчерпывающий обзор исследований по исследуемой проблеме и обширный список литературы по данной тематике. Считаю, что данная статья может быть допущена к публикации в журнале «Сибирские электронные математические известия».

Небольшие замечания по тексту:

1. Стр. 7, нужно определение класса **DP**.
2. Стр. 11: нужно более строгое определение класса **TFNP**.
3. Стр. 17, последний абзац: но тогда и «защитнику» тоже надо уметь решать задачу принадлежности множеству M для того, чтобы выбирать алгоритм защиты? То есть сложность множества M ударит и по защите. Или рецензент что-то не понял. Требуются пояснения.

Рецензент, 09.12.2025 г.