# ОТЗЫВ

на автореферат диссертации
***Прудникова Вадима Александровича,*** выполненной на тему
«Синтез и исследование псевдо-динамических подстановок», представленной на соискание ученой степени кандидата технических наук по научной специальности 2.3.6 «Методы и системы защиты информации, информационная безопасность»

Разработка эффективных и надёжных криптографических решений представляет собой ключевую проблему защиту данных современной информационной безопасности. Особую важность приобретает разработка алгоритмов, сочетающих как высокую производительность, так и энергоэффективность, что особенно критично для устройств с ограниченными вычислительными возможностями – мобильных и встраиваемых системы В данном аспекте, представленный в диссертационном исследовании метод синтеза псевдо–динамических подстановок на основе ARX-функций демонстрирует значительную практическую ценность и соответствует текущим требованиям отрасли.

Научная новизна диссертационного исследования заключается в создании оригинального метода синтеза псевдо–динамических подстановок на базе ARX-функций, позволяющего получать преобразования, удовлетворяющие всем требованиям по криптографическим свойствам, по затрачиваемым ресурсам и по скорости программной реализации криптографических преобразований. Этот факт подтверждается на практике, как теоретическими расчётами, так и экспериментально, в ходе испытаний.

Автореферат выполнен в соответствии с актуальными стандартами научных работ, характеризуется строгой структурой и логичной последовательностью изложения. Представленные результаты исследования содержат необходимый уровень детализации для объективной оценки их теоретической значимости и практической применимости.

По содержанию автореферата, можно указать на отдельные недостатки работы:

1. Из текста автореферата не ясен вклад «псевдо-динамичности» в PD–sbox, при условии, что основное преимущество PD–sbox перед фиксированными sbox – это устойчивость к статистическим методам криптоанализа за счёт динамики.

2. В содержании автореферата рисунки 3–5 не сопровождаются достаточно подробными пояснениями в тексте, что затрудняет их интерпретацию.

Обозначенные недостатки не относятся к вопросам, выносимым на защиту, и не влияют на положительную оценку автореферата и собственно диссертационной работы.

Диссертационная работа ***Прудникова Вадима Александровича*** «Синтез и исследование псевдо-динамических подстановок» вполне удовлетворяет требованиям, установленным Положением «О присуждении учёных степеней в федеральном государственном автономном образовательном учреждении высшего образования «Южный федеральный университет» (в действующей редакции) и предъявляемым к диссертациям на соискание учёной степени кандидата наук, а её автор, ***Прудников Вадим Александрович,*** вполне заслуживает присвоения ему учёной степени кандидата технических наук по специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность», технические науки.

Доктор физико–математических наук, доцент
(научная специальность – 01.04.03–Радиофизика)
профессор кафедры «Кибербезопасность информационных систем»
факультета «Информатика и вычислительная техника»
Донского государственного технического университета,

Черкесова Лариса Владимировна

03 июня 2025 г.

Подпись Черкесовой Ларисы Владимировны заверяю:
Учёный секретарь Учёного совета ДГТУ _____ В.Н. Анисимов

05 июня 2025 г.

Даю согласие на обработку персональных данных.

Место работы:
ФГБОУ ВО «Донской государственный технический университет»,
Адрес: 344000, г. Ростов–на–Дону, пл. Гагарина, 1; ауд. 1–326.
Кафедра «Кибербезопасность информационных систем»
Телефоны: +7(863) 273–27–16 (раб.), +7–989–536–00–25.
E–mail: chia2002@inbox.ru