ЗАКЛЮЧЕНИЕ ДИССЕРТАЦИОННОГО СОВЕТА ЮФУ801.02.02

созданного на базе федерального государственного автономного образовательного учреждения высшего образования «Южный федеральный университет» Минобрнауки России, по диссертации на соискание ученой степени кандидата наук

аттестационное дело № _____,
решение диссертационного совета
от 26 июня 2025 г. № 33

О присуждении **Прудникову Вадиму Александровичу**, гражданину Российской Федерации, ученой степени кандидата технических наук.

Диссертация «Синтез и исследование псевдо-динамических подстановок» по научной специальности 2.3.6 «Методы и системы защиты информации, информационная безопасность» принята к защите 23 апреля 2025 г. (протокол заседания № 32) диссертационным советом ЮФУ801.02.02, созданным на базе федерального государственного автономного образовательного учреждения высшего образования «Южный федеральный университет» в соответствии с приказами № 173-ОД от 30.06.2022 г., № 121-ОД от 28.04.2023 г.

Соискатель Прудников Вадим Александрович, 10.10.1996 года рождения, в 2020 г. окончил федеральное государственное автономное образовательное учреждение высшего образования «Южный федеральный университет» по специальности 10.05.02 «Информационная безопасность телекоммуникационных систем». В период подготовки диссертации с 2020 по 2024 гг. обучался в очной аспирантуре ФГАОУ ВО «Южный федеральный университет» по направлению подготовки 10.06.01 «Информационная безопасность», направленность образовательной программы – «Методы и системы защиты информации, информационная безопасность».

С 2024 г. по настоящее время работает в ФГАОУ ВО «Южный федеральный университет» в должности старшего преподавателя кафедры информационной безопасности телекоммуникационных систем Института компьютерных технологий и информационной безопасности.

Диссертация выполнена в федеральном государственном автономном образовательном учреждении высшего образования «Южный федеральный университет» на кафедре информационной безопасности телекоммуникационных систем Института компьютерных технологий и информационной безопасности.

Научный руководитель – **Румянцев Константин Евгеньевич**, доктор технических наук, профессор, федеральное государственное автономное образовательное учреждение высшего образования «Южный федеральный университет», заведующий кафедрой информационной безопасности телекоммуникационных систем.

Официальные оппоненты:

1. **Шелухин Олег Иванович**, доктор технических наук, профессор, Ордена Трудового Красного Знамени федеральное государственное бюджетное образовательное учреждение высшего образования «Московский технический университет связи и информатики», г. Москва, заведующий кафедрой «Информационная безопасность»;

2. **Панасенко Сергей Петрович**, кандидат технических наук, Акционерное общество «Актив-софт», г. Москва, директор по научной работе,

дали **положительные отзывы** на диссертацию.

Соискатель имеет 12 опубликованных научных работ, в том числе по теме диссертации опубликовано 11 научных печатных работ, из них 5 – в научных изданиях, входящих в Перечень рецензируемых научных изданий, в которых должны быть опубликованы основные научные результаты диссертаций на соискание ученой степени кандидата наук, на соискание ученой степени доктора наук, представленных для защиты в диссертационные советы Южного федерального университета (из них 1 – категории К1, RSCI, и 4 – категории К2); 6 – в материалах конференций и других научных печатных изданиях. По теме диссертации получено одно свидетельство о государственной регистрации программы для ЭВМ.

В диссертации отсутствуют недостоверные сведения об опубликованных

соискателем работах, в которых изложены основные научные результаты.

Наиболее значимые научные работы по теме диссертации:

1. Прудников, В. А. Анализ существующих подходов к синтезу псевдо-динамических sbox / В. А. Прудников // Вопросы кибербезопасности. – 2024. – № 4(62). – С. 57-64. – DOI 10.21681/2311-3456-2024-4-57-64. (Перечень ВАК, К1, RSCI, 100 % авторских). В работе Прудниковым В. А. проведён анализ существующих подходов к синтезу псевдо-динамических sbox.

2. Поликарпов, С. В. Синтез псевдо-динамических функций PD-sbox-ARX-32 / С. В. Поликарпов, В. А. Прудников, К. Е. Румянцев // Известия ЮФУ. Технические науки. – 2024. – № 5(241). – С. 102-118. – DOI 10.18522/2311-3103-2024-5-102-118. (Перечень ВАК, К2, 45% авторских). В работе Прудниковым В. А. разработан метод синтеза параметров 32-битной ARX-функции, получена количественная оценка затрачиваемых ресурсов программной реализации разработанного криптографического преобразования и криптографических свойств.

3. Поликарпов, С. В. Исследование свойств миниверсии псевдо-случайной функции pCollapser / С. В. Поликарпов, В. А. Прудников, К. Е. Румянцев // Известия ЮФУ. Технические науки. – 2022. – № 6(230). – С. 148-162. – DOI 10.18522/2311-3103-2022-6-148-162. (Перечень ВАК, К2, 40% авторских). В работе Прудниковым В. А. доказано, что использование псевдо-динамических подстановок на основе ARX-функций в PRF семейства pCollapser позволяет получить из набора 4 ARX-функций с предельно низкими криптографическими свойствами качественную нелинейную функцию, что подтверждает правильность работы псевдо-динамических подстановок PD-sbox.

4. Поликарпов, С. В. Вычислительно эффективный метод определения усреднённых линейных свойств псевдо-динамических подстановок / С. В. Поликарпов, В. А. Прудников, К. Е. Румянцев // Известия ЮФУ. Технические науки. – 2020. – № 5(215). – С. 16-30. – DOI 10.18522/2311-3103-2020-5-16-30. (Перечень ВАК, К2, 38% авторских). В работе Прудниковым В. А. разработан

вычислительно эффективный метод определения усреднённых линейных свойств псевдо-динамических подстановок для K-элементных PD-sbox.

5. Псевдослучайная функция pCollapser, обеспечивающая экстремальный параллелизм обработки информации / С. В. Поликарпов, В. А. Прудников, А. А. Кожевников, К. Е. Румянцев // Известия ЮФУ. Технические науки. – 2019. – № 5(207). – С. 88-100. – DOI 10.23683/2311-3103-2019-5-88-100. (Перечень ВАК, К2, 35% авторских). В работе Прудниковым В. А. разработана псевдо-случайная функция на основе PD-sbox – "pCollapser".

На диссертацию и автореферат поступило 8 отзывов. **Все отзывы положительные**. Во всех отзывах отмечено, что диссертационная работа соответствует паспорту научной специальности 2.3.6 «Методы и системы защиты информации, информационная безопасность», технические науки.

1) ФГАОУ ВО «Волгоградский государственный университет», г. Волгоград, отзыв подписал кандидат технических наук, доцент, заведующий кафедрой телекоммуникационных систем Семенов Евгений Сергеевич, 3 замечания;

2) ФГБОУ ВО «Иркутский государственный университет путей сообщения», г. Иркутск, отзыв подписал доктор технических наук, доцент, профессор кафедры «Информационные системы и защита информации» Аршинский Леонид Вадимович, 1 замечание;

3) ФГБОУ ВО «Донской государственный технический университет», г. Ростов-на-Дону, отзыв подписала доктор физико-математических наук, доцент, профессор кафедры «Кибербезопасность информационных систем» Черкесова Лариса Владимировна, 2 замечания;

4) ФГБОУ ВО «Московский энергетический институт (национальный исследовательский университет)», Институт информационных и вычислительных технологий, г. Москва, отзыв подписал доктор технических наук, профессор, профессор кафедры управления и интеллектуальных технологий Филаретов Геннадий Федорович, 2 замечания;

5) ФГАОУ ВО «Севастопольский государственный университет», г. Севастополь, отзыв подписал кандидат технических наук, заведующий кафедрой «Информационная безопасность» Ожиганова Марина Ивановна, 2 замечания;

6) ФГБОУ ВО «Чеченский государственный университет им. А.А. Кадырова», г. Грозный, отзыв подписал кандидат технических наук, и.о. заведующего кафедрой программирования и инфокоммуникационных технологий, и.о. директора института математики, физики и информационных технологий Дахкильгова Камила Багаудиновна, 2 замечания;

7) ФГАОУ ВО «Северо-Кавказский федеральный университет», г. Ставрополь, отзыв подписал кандидат технических наук, профессор, профессор кафедры организации и технологии защиты информации Жук Александр Павлович, 2 замечания;

8) ФГБОУ ВО «Российский государственный гидрометеорологический университет», г. Санкт-Петербург, отзыв подписал доктор технических наук, доцент, профессор кафедры информационных технологий и систем безопасности Лепешкин Олег Михайлович, 2 замечания.

Наиболее существенные замечания:

1. В тексте автореферата представлен универсальный метод синтеза PD-sbox-ARX для микроконтроллеров семейства AVR, однако его важный начальный этап эвристического выбора структуры ARX-функции с учётом особенностей программной и аппаратной реализации не формализован, что не позволяет понять, насколько он зависит от опыта и интуиции исследователя.

2. В тексте автореферата представлено сравнение разработанной подстановки PD-sbox-ARX с такими криптографическими преобразованиями, как miniAlzette32 (Alzette-подобная структура) и 8 раундов криптоалгоритма Speck32. Не ясно, проводилось ли сравнение PD-sbox-ARX с малоресурсными реализациями отечественных криптоалгоритмов «Кузнечик» или «Магма». Если нет, то чем это аргументировано?

Выбор официальных оппонентов обосновывается их достижениями в

данной отрасли науки и способностью определить научную и практическую ценность диссертации. Доктор технических наук Шелухин Олег Иванович, профессор, Заслуженный деятель науки РФ, заведующий кафедрой «Информационная безопасность» федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики» является ведущим специалистом в области информационной безопасности, имеет необходимое количество публикаций в рецензируемых ведущих научных журналах по тематике диссертации. Кандидат технических наук Панасенко Сергей Петрович, директор по научной работе Акционерного общества «Актив-софт», является известным специалистом в области информационной безопасности и блокчейн-технологий, автором шести книг и более 300 научных публикаций по криптографии и защите информации. Имеет более 10 патентов.

Диссертационный совет отмечает, что на основании выполненных соискателем исследований получены следующие научные результаты, обладающие новизной и свидетельствующие о личном вкладе соискателя:

– разработан метод синтеза параметров 32-битной ARX-функции PD-sbox-ARX, **отличающийся** от случайного подбора параметров эффективным использованием ресурсов и особенностей процессоров, а также основным критерием синтеза ARX-функций, заключающимся в использовании сдвигов, кратных 8 бит, и параллельностью выполнения представленных в ней операций. Разработанный метод **позволяет** получить параметры операций циклического сдвига, при которых обеспечивается минимальное количество затрачиваемых ассемблерных инструкций на операции циклического сдвига при реализации на 8-битных микроконтроллерах и обеспечиваются криптографические свойства качественной нелинейной функции с максимальным весом разностной характеристики, равным 2^{-32}, и линейным 2^{-13} для результирующего PD-sbox-ARX, состоящего из четырёх 32-битных ARX-функций (пункт 19 паспорта специальности);

– разработана структура псевдо-динамической операции подстановки на основе ARX-функций, **отличающихся** от существующих параллельностью выполняемых операций и новыми связями между структурными элементами ARX-функции. Разработанная структура обладает свойствами эквивалентных замен аналогичными случайно сформированным операциям подстановки той же размерности и **позволяет** получить из набора 4 ARX-функций с предельно низкими криптографическими свойствами качественную нелинейную функцию (пункт 19 паспорта специальности).

В диссертации содержится **решение актуальной научной задачи** – разработка и исследование метода синтеза псевдо-динамических подстановок на основе ARX-функций, удовлетворяющих широкому спектру противоречивых требований по стойкости к криптоанализу и затрачиваемым ресурсам при программной реализации криптографических преобразований. Предложенные автором диссертации решения научно обоснованы и оценены по сравнению с другими известными решениями.

Теоретическая значимость исследования обоснована тем, что **доказаны** основные научные положения, выносимые на защиту, вносящие вклад в развитие перспективного научного направления синтеза и применения псевдо-динамических подстановок на основе ARX-функций, удовлетворяющих широкому спектру противоречивых требований по стойкости к криптоанализу и затрачиваемым ресурсам при программной реализации криптографических преобразований.

Значение полученных соискателем результатов исследования для практики подтверждается тем, что применение псевдо-динамических подстановок на базе подобранных ARX-функций, обладающих дифференциальными и линейными свойствами эквивалентных подстановок, аналогичными случайно сформированным фиксированным подстановкам той же размерности, позволяет обеспечить критический путь (максимальное количество последовательных операций сложения по модулю 2^{16}) в четыре раза меньше, чем 8-итерационная 32-битная Alzette-подобная структура, при двукратном

увеличении количества операций и при сопоставимых максимальных значениях весов разностных и линейных характеристик. При аппаратной реализации ARX-функции данное свойство позволяет пропорционально уменьшить (до 4 раз) задержку при преобразовании блоков информации.

Результаты диссертации использованы:

– при подаче заявки «Метод синхронизации между абонентами локальной квантовой сети и доверенным узлом магистральной квантовой сети» на конкурс 2024 года Российского научного фонда «Проведение фундаментальных научных исследований и поисковых научных исследований малыми отдельными научными группами». В частности, формулирование частной научной задачи гранта, связанной с поиском возможных контрмер против выявленных атак, основывается на научных результатах диссертационной работы в части метода синтеза псевдо-динамической подстановки PD-sbox-ARX-32 и структуры псевдо-динамической операции подстановки на основе ARX-функций. Применение результатов отражено в акте о внедрении, утвержденном директором Института компьютерных технологий и информационной безопасности ФГАОУ ВО «Южный федеральный университет» Веселовым Г. Е. от 04.02.2025;

– в научно-исследовательской работе кафедры информационной безопасности телекоммуникационных систем Института компьютерных технологий и информационной безопасности ФГАОУ ВО «Южный федеральный университет» в рамках выполнения инициативной научно-исследовательской работы «Метод синтеза псевдо-динамических операций подстановки с предельными криптографическими характеристиками для семейства перспективных легковесных псевдослучайных функций pCollapser». Применение результатов отражено в акте о внедрении, утвержденном директором Института компьютерных технологий и информационной безопасности ФГАОУ ВО «Южный федеральный университет» Веселовым Г. Е. от 16.01.2024;

– в учебном процессе кафедры информационной безопасности телекоммуникационных систем Института компьютерных технологий и информационной безопасности ФГАОУ ВО «Южный федеральный университет» для подготовки студентов специальности 10.05.02 «Информационная безопасность телекоммуникационных систем» в рамках дисциплины «Разработка программно-аппаратных средств телекоммуникационных систем». Применение результатов отражено в акте о внедрении, утвержденном директором Института компьютерных технологий и информационной безопасности ФГАОУ ВО «Южный федеральный университет» Веселовым Г. Е. от 04.04.2024.

Оценка достоверности результатов исследования выявила, что результаты обоснованы сходимостью исходной гипотезы с результатами опытно-экспериментальных данных, а также строгостью применяемого математического аппарата. Теория построена на известных, проверяемых данных и согласуется с опубликованными экспериментальными данными по теме диссертации. Установлено качественное и количественное совпадение авторских результатов с результатами, представленными в независимых источниках по тематике диссертации.

Личный вклад соискателя состоит в том, что основные научные результаты, в том числе структура псевдо-динамической операции подстановки на основе ARX-функций, метод синтеза параметров 32-битной ARX-функции PD-sbox-ARX, а также количественная оценка затрачиваемых ресурсов программной реализации разработанного криптографического преобразования и криптографических свойств получены автором лично.

В ходе защиты диссертации были высказаны следующие критические замечания:

1. В работе не проанализированы потенциальные уязвимости PD-sbox-ARX-32 к иным криптографическим атакам, например, алгебраическим или атакам по сторонним каналам. Диссертантом не обоснован отказ от анализа таких криптографических атак для представленной подстановки.

2. Сравнивали ли вы, с точки зрения результирующего порядка нелинейности, известные подстановки, например из криптоалгоритма AES, с порядком нелинейности, который получается при использовании ваших подстановок?

Соискатель Прудников Вадим Александрович ответил на задаваемые ему в ходе заседания вопросы и привел собственную аргументацию:

1. С замечанием согласен. В ходе диссертационного исследования выполненный линейный и разностный криптоанализ PD-sbox-ARX показал криптографические свойства качественной нелинейной функции.

2. С замечанием согласен. В результатах диссертационных исследований не представлено сравнение с существующими подстановками с точки зрения результирующего порядка нелинейности. В публикациях по данной тематике соответствующие материалы представлены.

Диссертация Прудникова Вадима Александровича является завершенной научно-квалификационной работой, обладающей теоретической новизной и практической значимостью, внутренним единством, содержит новые научные результаты и положения, свидетельствующие о личном вкладе автора.

В диссертации отсутствуют заимствования без ссылок на авторов или источник заимствования. Приведены ссылки на все использованные в диссертации результаты научных работ, выполненные соискателем лично и в соавторстве.

На заседании 26 июня 2025 г. диссертационный совет отметил, что рассматриваемая диссертация соответствует критериям раздела 2 «Положения о присуждении ученых степеней в федеральном государственном автономном образовательном учреждении высшего образования «Южный федеральный университет» (в редакции от 29.03.2024 г. приказ № 66-ОД), и постановил за решение актуальной научной задачи, имеющей значение для развития соответствующей отрасли знаний, присудить **Прудникову Вадиму Александровичу** ученую степень **кандидата** технических наук по научной специальности 2.3.6 «Методы и системы защиты информации, информационная

безопасность».

При проведении тайного голосования диссертационный совет в количестве 8 человек, из них 7 докторов наук по научной специальности 2.3.6 «Методы и системы защиты информации, информационная безопасность», участвовавших в заседании, из 10 человек, входящих в состав совета, дополнительных членов в состав совета не вводилось, проголосовали:

за – 8, против – нет , недействительных бюллетеней – нет.

Председатель диссертационного совета **Бабенко Людмила Клементьевна**

Ученый секретарь диссертационного совета 26 июня 2025 г. **Ельчанинова Наталья Борисовна**