

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Объект авторского права
УДК 519.65

БУРДЕЛЁВ
Александр Владимирович

**Пороговые k -значные функции, их характеристика и применение в
системах защиты информации**

Автореферат
диссертации на соискание ученой степени
кандидата физико-математических наук
по специальности
05.13.19 «Методы и системы защиты информации,
информационная безопасность»

Научная работа выполнена в Белорусском государственном университете и Федеральном государственном казенном научном учреждении «Академия криптографии Российской Федерации»

Научный руководитель

Никонов Владимир Глебович,

доктор технических наук, профессор, член-корреспондент Академии криптографии Российской Федерации, ведущий научный сотрудник лаборатории №5 Научно-исследовательского центра Академии криптографии Российской Федерации

Официальные оппоненты:

Тузиков Александр Васильевич,

доктор физико-математических наук, профессор, член-корреспондент НАН Беларуси, заведующий лабораторией ГНУ «Объединенный институт проблем информатики НАН Беларуси»

Волошко Валерий Анатольевич,

кандидат физико-математических наук, заведующий сектором учреждения БГУ «Научно-исследовательский институт прикладных проблем математики и информатики»

Оппонирующая
организация

ГНУ «Институт математики Национальной академии наук Беларуси»

Защита состоится 6 марта 2025 года в 14:30 на заседании совета по защите диссертаций Д 02.01.02 при Белорусском государственном университете по адресу: 220030, Республика Беларусь, г. Минск, ул. Ленинградская, 8 (корпус юридического факультета), ауд. 407, тел. учёного секретаря: 209-52-04; e-mail: kochyn@bsu.by.

С диссертацией можно ознакомиться в Фундаментальной библиотеке Белорусского государственного университета.

Автореферат разослан « 21 » января 2025 г.

Учёный секретарь совета
по защите диссертаций



В.П.Кочин

ВВЕДЕНИЕ

В диссертации исследуются пороговые k -значные функции в связи с их применением в системах защиты информации, и изучается проблема построения аналитического задания произвольной пороговой k -значной функции, известная также как проблема характеристики пороговой k -значной функции. Применение пороговых функций в системах защиты информации объясняется простотой их технической реализации, согласованностью с логикой выполнения важнейших операций при обработке дискретной информации, высоким быстродействием и применением в нейροкомпьютерах. С методологической точки зрения данное исследование представляет интерес также в связи с развитием нейрокомпьютеров как новой вычислительной среды^{1, 2, 3}.

Пороговая функция базируется на вычислении скалярного произведения на множестве действительных чисел и сравнения полученного результата с фиксированным порогом. Вычисление скалярного произведения является базовой операцией всех вычислительных платформ, как традиционных, так и перспективных^{1, 2, 3, 4, 5}. Встроенность этой операции во внутреннюю логику ЭВМ делает пороговую функцию исключительно удобным базовым элементом, который получил широкое распространение и в универсальных, и в специальных вычислительных средствах^{3, 6, 7}.

Внимание к изучению возможных приложений пороговых функций в немалой степени было инициировано также обнаружением пороговой природы работы нейронов живых организмов. В опубликованной в 1943 году работе⁸ У. Маккалока и У. Питтса, на основании экспериментальных данных была построена модель так называемого формального нейрона, которая описывала работу нейронов с помощью булевых пороговых функций. Тот факт, что именно пороговые операции были отобраны природой в качестве базиса для выполнения высших функций мозга, явился исходным пунктом для широкого развития одного из важнейших направлений современной прикладной бионики —

¹ Розенблатт, Ф. Принципы нейродинамики. Перцептроны и теория механизмов мозга / Ф. Розенблатт ; пер. с англ. / В. Я. Алтаева [и др.] ; под ред. С. М. Осовца, — Москва : Мир, 1965. — 480 с.

² Бутаков, Е. А. Методы синтеза релейных устройств из пороговых элементов / Е. А. Бутаков. — М. : Энергия, 1970. — 328 с.

³ Миркес, Е. М. Функциональные модели универсального нейрокомпьютера: дисс. ... д-ра техн. наук: 05.13.11 / Е. М. Миркес. — Красноярск, 2001. — 418 л.

⁴ Дертоузос М. Пороговая логика / М. Дертоузос. — Москва: Мир, 1967. — 342 с.

⁵ Widrow, B. Adaptive Switching Circuits / B. Widrow, M. E. Hoff. // IRE WESTCON Convention Record. — 1960. — Part 4. — P. 96–104.

⁶ Минский, М. Перцептроны // М. Минский, С. Паперт — Москва: Мир, 1971. — 261 с.

⁷ Hopfield, J. J. Neural networks and physical systems with emergent collective computational abilities / J. J. Hopfield // Proc. Natl. Acad. Sci. USA. — 1982. — Vol. 79, Issue 8. — P. 2554–2558.

⁸ McCulloch, W.S. A logical calculus of the ideas immanent in nervous activity / W.S. McCulloch, W. Pitts // A Bulletin of Mathematical Biophysics. — 1943. — Vol. 5. — P. 115–133.

построению так называемых нейрокомпьютеров^{1, 8, 9, 10}. Несмотря на обилие исследований в этой области, необходимо констатировать, что проблеме анализа реализуемых в нейрокомпьютере преобразований и защите данных в нейросетях уделяется мало внимания. Возникающие при этом задачи объективно сводятся к распознаванию пороговых элементов, их характеристике, причем не только в булевом, но и в k -значном случаях. Необходимость перехода в k -значную логику определилась благодаря обнаруженной уточненной природе нейронов, логика работы которых отвечает не булевым, а пороговым k -значным функциям⁹. Изучение пороговых k -значных функций и построенных на их основе сетей сделало заявленную проблему диссертации – характеристику пороговых k -значных функций – актуальной и практически значимой в своей прямой постановке.

Переход к переработке и передаче информации на новых физических принципах с высоким быстродействием стал ещё одним источником повышенного интереса к изучению базиса пороговых k -значных функций. В частности, использование оптических каналов связи и оптической вычислительной среды делает^{11, 12} базис, состоящий из пороговых функций, самым удобным и согласованным с логикой переработки такой информации. Обращение к оптическим методам переработки и передачи информации, таким образом, также делает рассматриваемую в диссертации проблему характеристики пороговой k -значной функции актуальной и практически значимой.

Вместе с тем необходимо отметить, что в булевом случае данная задача известна достаточно давно^{1, 4} и её решению были посвящены работы многих авторов^{1, 2, 4, 13, 14}. Несмотря на известную простоту её постановки, задача проверки принадлежности конкретной функции классу пороговых функций и нахождения её аналитического задания оказалась достаточно сложной. В случае если функция действительно оказывалась пороговой, для нахождения её порогового представления предполагалась определенная итеративная

⁹ Вальцев, В. Б. Некоторые структурные принципы организации высших функций мозга / В. Б. Вальцев, В. Р. Григорьев, В. Г. Никонов // «Нейрокомпьютер как основа мыслящих ЭВМ». – М.: Наука. – 1993. – с. 38–46.

¹⁰ Терехин, А. Т. Нейросетевое моделирование когнитивных функций мозга: обзор основных идей / А. Т. Терехин, Е. В. Будилова, Л. М. Качалова, М.П. Карпенко // Психологические исследования: электрон. журн. – 2009. – N 2(4). – Режим доступа: <https://psystudy.ru/index.php/num/article/view/997/532> – Дата доступа: 2024.05.23.

¹¹ Белов П. А., Беспалов В. Н. и др. Оптические процессоры: достижения и новые идеи // Проблемы когерентной и нелинейной оптики. – СПб., 2006.

¹² Jahns J., Lee S. H. Optical Computing Hardware: Optical Computing // Elsevier Science, 1993.

¹³ Chow, C. On the characterization of threshold functions. / C. Chow // In Proceedings of the Symposium on Switching Circuit Theory and Logical Design (FOCS). – 1961. – P. 34–38.

¹⁴ Беляков-Бодин В. И., Розенблит С. И. Исследование некоторых вопросов синтеза пороговых функций // - М. Институт теоретической и экспериментальной физики Гос. Комитета по использованию атомной энергии СССР, 1972.

процедура. Разумеется, переход в k -значную ($k > 2$) логику сопряжен с усложнением и развитием этих подходов.

Задача характеристики пороговых булевых и k -значных функций, сводящаяся¹⁵ к решению систем линейных неравенств, приобрела¹⁶ полиномиальную сложность благодаря результату Л. Хачияна. Высокая трудоемкость каждой итерации алгоритма эллипсоидов и их большое число оставили актуальной проблему поиска алгоритмов, менее трудоемких, чем алгоритм Хачияна. Отмеченная актуальность проблемы характеристики пороговых k -значных функций привлекла других авторов. Наиболее известной здесь оказалась работа З. Обрадовича¹⁷.

Теоретическая значимость данной диссертации заключается в построении нового алгоритма характеристики и доказательстве его сходимости за конечное число шагов. Ещё одним важным результатом диссертации стал тот факт, что построенный в ней геометрический алгоритм по всем параметрам улучшает алгоритм Обрадовича. Это стало возможным благодаря включению в геометрический алгоритм начальных параметров, в известном смысле обобщающих параметры Чоу¹³ на случай k -значной логики, и оригинального геометрического метода их корректировки.

Актуальность темы диссертации определяется проходящим в настоящее время переходом на высокоскоростную передачу информации по современным и перспективным каналам связи, в частности оптическим, требующим разработки соответствующих систем защиты информации высокого быстродействия.

Проблема характеристики пороговых функций известна давно, с 60-х годов прошлого века, но она изучалась лишь для булевых функций. С наибольшей полнотой эта проблема рассматривалась в работах^{1, 2, 4, 14}, для её решения, использовались параметры Чоу для первого приближения коэффициентов искомой линейной формы. Первые публикации по характеристике пороговых k -значных функций появились в 2000-х годах^{16, 18, 19}. Это работы таких авторов как З. Обрадович, А. Нгом, М. Энтони, результаты которых служат отправной точкой для диссертационного исследования.

¹⁶ Хачиян Л. Г. Полиномиальные алгоритмы в линейном программировании // ЖВМиМФ, 1980, вып. 20, №1, с. 51–68.

¹⁷ Obradovic Z. Learning with Discrete Multi-Valued Neurons // Machine Learning: Proc. 7th Int'l. Conf., 1990, ed. B. W. Porter and R.J. Mooney, Austin, TX, Morgan-Kaufmann, pp. 392–399.

¹⁸ Ngom A. Synthesis of Multiple-Valued Logic Functions by Neural Networks // Ph.D. Thesis Dissertation, Computer Science Department, University of Ottawa, Ontario, October 1998.

¹⁹ Anthony M. Learning Multivalued Multithreshold Functions // CDAM Research Report LSE-CDAM-2003-03, January 2003.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Связь работы с научными программами (проектами), темами

Тема диссертации соответствует направлениям научных исследований, определенным Перечнем приоритетных направлений научных исследований Республики Беларусь «Методы, средства и технологии обеспечения информационной безопасности при обработке, хранении и передаче данных с использованием криптографии, квантово-криптографические системы» (2011–2015 годы), «Безопасность человека, общества и государства» (2016–2020 годы) и «Средства технической и криптографической защиты информации, криптология и кибербезопасность» (2021–2025 годы).

Цель и задачи, объект и предмет исследования

Цель диссертации – анализ комбинаторных свойств пороговых k -значных функций, разработка и анализ алгоритмов характеристики пороговой k -значной функции, позволяющих оценивать её параметры по столбцу значений.

Для достижения поставленной цели требуется решить следующие основные задачи:

1. Построение функционалов близости и отличия функций k -значной логики, аппроксимирующих коэффициенты линейной формы, для характеристики пороговой k -значной функции, и доказательство их свойств.

2. Разработка нового геометрического алгоритма характеристики пороговой k -значной функции на основе построенных функционалов и доказательство его сходимости за конечное число шагов.

3. Экспериментальное исследование свойств геометрического алгоритма характеристики, сравнение его характеристик с характеристиками алгоритма Обрадовича и алгоритма на основе метода эллипсоидов Хачияна; и разработка модификации геометрического алгоритма.

4. Применение разработанного геометрического алгоритма для решения задач анализа и синтеза узлов усложнения в системах защиты информации.

Объектом исследования являются пороговые k -значные функции, их способы задания, параметры и свойства. *Предметом исследования* являются методы характеристики пороговых k -значных функций.

Научная новизна

Научная новизна диссертации заключается в принципиальной новизне разработанных в диссертации алгоритмов характеристики пороговых k -значных функций. Новыми являются и введенные характеристики: коэффициенты роста и возрастания, используемые для задания пороговой k -значной функции. Оригинальность построенного модифицированного геометрического алгоритма состоит в гибридном подходе к проблеме характеристики пороговых k -значных

функций, позволяющем осуществить балансирование между числом итераций алгоритма и числом обращений к вычислению значений функции. Новым является метод восстановления пороговой k -значной функции в узле защиты информации по неполным данным с помощью разработанного алгоритма характеристики.

Положения, выносимые на защиту

1. Теоретически доказанные и экспериментально установленные свойства функционалов близости и отличия функций k -значной логики, аппроксимирующих коэффициенты линейной формы.

2. Новый геометрический алгоритм характеристики пороговой k -значной функции и его модификация, направленная на снижение числа обращений к вычислению значений искомой функции.

3. Доказательство сходимости разработанного геометрического алгоритма характеристики пороговой k -значной функции и его модификации за конечное число шагов.

4. Результаты сравнительного анализа характеристик геометрического алгоритма и его модификации с характеристиками алгоритма Обрадовича и алгоритма на основе метода эллипсоидов Хачияна, демонстрирующие превосходство разработанных алгоритмов. При $k > 4$ построенные алгоритмы дают преимущество в числе итераций алгоритма более чем в 10^3 раз, и с увеличением k и n это преимущество возрастает.

5. Результаты компьютерного моделирования геометрического алгоритма и его применения для решения задач анализа и синтеза узлов усложнения в системах защиты информации.

Личный вклад соискателя ученой степени

Основные результаты диссертационной работы получены соискателем самостоятельно. Научному руководителю в совместных работах принадлежат выбор направления исследований, предметные постановки задач, обсуждение результатов. Результаты, полученные другими соавторами или с другими соавторами, не вошли в диссертацию.

Апробация диссертации и информация об использовании ее результатов

Результаты диссертации прошли апробацию на научном семинаре кафедры математического моделирования и анализа данных Белорусского государственного университета (г. Минск, 10 октября 2017 г.); на конференции WebConf2018 «Веб-программирование и интернет-технологии» (г. Минск, 14–18 мая 2018 г.); XXVIII научно-практической конференции «Комплексная защита информации» (г. Гомель, 23–25 мая 2023 г.). Разработанные методы характеристики пороговых k -значных функций и их применение в задачах

защиты информации внедрены в лекционный курс, читаемый автором на кафедре математического моделирования и анализа данных факультета прикладной математики и информатики Белорусского государственного университета, что подтверждено актом внедрения. Также результаты диссертационной работы использованы для разработки программно-аппаратного комплекса ООО «Линфо» (г. Москва, Российская Федерация) и в исследованиях по специальной тематике в/ч 03405 (г. Минск, Республика Беларусь).

Опубликованность результатов диссертации

Основные результаты диссертационной работы опубликованы в 10 научных работах, из которых: 5 статей в научных изданиях в соответствии с п. 19 Положения о присуждении ученых степеней и присвоении ученых званий (общий объем 3,59 авторского листа), 3 статьи в других научных изданиях, 2 материалов конференций и тезисов докладов.

Структура и объем диссертации

Диссертация состоит из перечня сокращений и обозначений, введения, общей характеристики работы, четырех глав, заключения, списка литературы и Приложений, содержащих таблицы экспериментальных результатов оценивания трудоемкости разработанных алгоритмов и акты внедрения результатов диссертационного исследования. Полный объем диссертации составляет 131 страницу, в том числе 13 рисунков занимают 5 страниц, 21 таблица на 11 страницах, четыре приложения занимают 9 страниц. Список использованных источников содержит 96 наименований, включая собственные публикации соискателя ученой степени (на 9 страницах).

ОСНОВНАЯ ЧАСТЬ

В главе 1 введены определения пороговых булевых и k -значных функций, рассмотрены их основные свойства и осуществлен исторический обзор развития вопроса изучения данных классов функций.

В разделе 1.1 рассмотрены булевы пороговые функции и история их изучения. В числе прочего рассмотрены вопросы их однородности, монотонности, самодвойственности, наличия запретов и сложности взаимной перестройки пороговых булевых функций. Приведены оценки числа пороговых функций, размаха пороговой булевой функции. Изложены основные методы распознавания пороговости булевой функции, свойства коэффициентов Чоу. Выделены наиболее изученные классы пороговых булевых функций: мажоритарные, равновероятные и линейно-разделимые.

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ УЧЕНОЙ СТЕПЕНИ

Статьи в научных изданиях в соответствии с п. 19 Положения о присуждении ученых степеней и присвоении ученых званий

1-А. Бурделёв, А. В. Распознавание параметров узла защиты информации, реализованного пороговой k -значной функцией / А. В. Бурделёв, В. Г. Никонов, И. И. Лапиков // Труды СПИИРАН. – 2016. – Вып. 46. – С. 108–127.

2-А. Бурделёв, А. В. Сравнительный анализ геометрического алгоритма и модифицированного метода эллипсоидов в задаче распознавания параметров узла защиты информации, реализованного k -значной пороговой функцией / А. В. Бурделёв, И. И. Лапиков // Интернет-журнал «Науковедение». – 2017. – Т. 9, №6. С. загл. с экрана.

3-А. Бурделёв, А. В. О свойствах коэффициентов роста и коэффициентов возрастания / А. В. Бурделёв // Лесной вестник / Forestry bulletin. – 2017. – Т. 21, Вып. 6. – С. 101–108.

4-А. Бурделёв, А. В. О сходимости нового алгоритма характеристики k -значных пороговых функций / А. В. Бурделёв // Прикладная дискретная математика. – 2018. – №39. – С. 107–115.

5-А. Бурделёв, А. В. Восстановление аналитического задания пороговой k -значной функции в узле защиты информации при неполных данных. / А. В. Бурделёв // Журнал Белорусского государственного университета. Математика. Информатика. – 2023. – №3. – С. 63–71.

Статьи в других научных изданиях

6-А. Бурделёв, А. В. О построении аналитического задания k -значной пороговой функции / А. В. Бурделёв, В. Г. Никонов // Computational nanotechnology – 2015. – Вып. 2. – С. 5–13.

7-А. Бурделёв, А. В. О новом алгоритме характеристики k значных пороговых функций / А. В. Бурделёв, В. Г. Никонов // Computational nanotechnology. – 2017. – Вып. 1. – С. 7–14.

8-А. Бурделёв, А. В. Модификация геометрического алгоритма характеристики пороговых k -значных функций / А. В. Бурделёв // Computational nanotechnology. – 2018. – Вып. 1. – С. 132–138.

Материалы конференций и тезисы докладов

9-А. Бурделёв, А. В. Пороговые k -значные функции, их характеристика и применение в системах защиты информации / А. В. Бурделёв // Веб-программирование и интернет-технологии WebConf2018: тез. докл.

4-й Междунар. науч.-практ. конф., Минск, 14–18 мая 2018 г. / Белорус. гос. ун-т; редкол.: И. М. Галкин (отв. ред.) [и др.]. – Минск, 2018. – С. 150.

10-А. Бурделёв, А. В. Восстановление аналитического задания пороговой k-значной функции в узле защиты информации при неполных данных / А. В. Бурделёв // Комплексная защита информации: материалы XXVIII научно-практической конференции, Гомель, 23-25 мая 2023 г. / УГЗ МЧС Республики Беларусь. – Минск, 2023. – С. 212–216.

РЭЗЮМЭ

Бурдзялёў Аляксандр Уладзіміравіч

Парогавыя k -знакавыя функцыі, іх характарызацыя і прымяненне ў сістэмах абароны інфармацыі

Ключавыя словы: парогавая k -значная функцыя, каэфіцыенты росту, каэфіцыенты ўзрастання, геаметрычны алгарытм характарызацыі парогавай k -значнай функцыі, збежнасць алгарытму, вузел абароны інфармацыі, алгарытм Абрадавіча, параметры Намуры.

Мэта працы: аналіз камбінаторных уласцівасцяў парогавых k -значных функцый, распрацоўка і аналіз алгарытмаў характарызацыі парогавай k -значнай функцыі, якія дазваляюць ацэньваць яе параметры.

Метады даследвання: дыскрэтная матэматыка, тэорыя булевых функцый і функцый k -значнай логікі, матэматычны аналіз, аналітычная геаметрыя, тэорыя верагоднасцяў, абарона інфармацыі, тэорыя алгарытмаў з ужываннем матэматычнага мадэлявання і кампутарных эксперыментаў.

Атрыманыя вынікі і іх навізна. У выніку праведзеных у дысертацыі даследаванняў пабудаваны новы геаметрычны алгарытм характарызацыі парогавых k -значных функцый, які выкарыстоўвае асаблівасці геаметрычнай будовы, а таксама ўведзены каэфіцыенты росту і ўзрастання. Тэарэтычна даказана збежнасць гэтага алгарытму за канчатковы лік крокаў. Параўнальны аналіз новага пабудаванага алгарытму і яго мадыфікацыі з алгарытмам Абрадавіча і алгарытмам на аснове метаду эліпсоідаў Хачыяна паказвае перавагу геаметрычнага алгарытму па характарыстыках працаёмкасці.

Рэкамендацыі па выкарыстанні. Атрыманыя ў дысертацыі вынікі накіраваны на выкарыстанне ў задачах аналізу і сінтэзы сістэм крыптаграфічнай абароны інфармацыі высокай хуткадзейнасці. Вынікі дысертацыі могуць быць выкарыстаны ў практычных задачах аднаўлення параметраў вузла абароны інфармацыі, рэалізаванага парогавай k -значнай функцыяй, а таксама ў задачы аднаўлення аналітычнага задання парогавай функцыі ўскладнення пры няпоўных дадзеных. Вынікі дысертацыі скарыстаны ў практычных задачах абароны інфармацыі і ў навучальным працэсе.

Галіна прымянення: абарона інфармацыі, дыскрэтная матэматыка.

РЕЗЮМЕ

Бурделёв Александр Владимирович**Пороговые k -значные функции, их характеристика и применение в системах защиты информации**

Ключевые слова: пороговая k -значная функция, коэффициенты роста, коэффициенты возрастания, геометрический алгоритм характеристики пороговой k -значной функции, сходимость алгоритма, узел защиты информации, алгоритм Обрадовича, параметры Номуры

Цель работы: анализ комбинаторных свойств пороговых k -значных функций, разработка и анализ алгоритмов характеристики пороговой k -значной функции, позволяющих оценивать её параметры.

Методы исследования: дискретная математика, теория булевых функций и функций k -значной логики, математический анализ, аналитическая геометрия, теории вероятностей, защита информации, теория алгоритмов с применением математического моделирования и компьютерных экспериментов.

Полученные результаты и их новизна. В результате проведенных в диссертации исследований построен новый геометрический алгоритм характеристики пороговых k -значных функций, использующий особенности геометрического строения, а также введены коэффициенты роста и возрастания. Теоретически доказана сходимость этого алгоритма за конечное число шагов. Сопоставительный анализ нового построенного алгоритма и его модификации с алгоритмом Обрадовича и алгоритма на основе метода эллипсоидов Хачияна показывает превосходство геометрического алгоритма по характеристикам трудоемкости.

Рекомендации по использованию. Полученные в диссертации результаты направлены на использование в задачах анализа и синтеза систем криптографической защиты информации высокого быстродействия. Результаты диссертации могут быть использованы в практических задачах восстановления параметров узла защиты информации, реализованного пороговой k -значной функцией, а также в задаче восстановления аналитического задания пороговой функции усложнения при неполных данных. Результаты диссертации использованы в практических задачах защиты информации и в учебном процессе.

Область применения: защита информации, дискретная математика.

SUMMARY

Burdeliov Alexander Vladimirovich**Threshold k-valued functions, their characterization and application in information security systems**

Key words: threshold k-valued function, growth coefficients, increasing coefficients, geometric algorithm for characterizing the threshold k-valued function, convergence of the algorithm, information security node, Obradovic algorithm, Nomura parameters.

Purpose of the work: analysis of combinatorial properties of threshold k-valued functions, development and analysis of algorithms for characterizing a threshold k-valued function, allowing to estimate its parameters.

Research methods: discrete mathematics, theory of Boolean functions and k-valued logic functions, mathematical analysis, analytical geometry, probability theories, information security, theory of algorithms using mathematical modeling and computer experiments.

Obtained results and their novelty. As a result of the research carried out in the dissertation, a new geometric algorithm for characterizing threshold k-valued functions was constructed, using the features of the geometric structure, and growth and increase coefficients were introduced. The convergence of this algorithm in a finite number of steps has been theoretically proven. A comparative analysis of the new constructed algorithm and its modification with the Obradovic algorithm and the algorithm based on the Khachiyan ellipsoid method shows the superiority of the geometric algorithm in terms of labor intensity characteristics.

Recommendations for use. The results obtained in the dissertation are aimed at using high-performance cryptographic information protection systems in problems of analysis and synthesis. The results of the dissertation can be used in practical problems of restoring the parameters of an information security unit implemented by a threshold k-valued function, as well as in the problem of restoring the analytical task of a threshold complication function with incomplete data. The results of the dissertation are used in practical problems of information security and in the educational process.

Area of application: information security, discrete mathematics.



Подписано в печать 13.01.2025. Формат 60×84 $\frac{1}{16}$. Бумага офсетная.
Ризография. Усл. печ. л. 1,39. Уч.-изд. л. 1,5.
Тираж 60 экз. Заказ 2.

Отпечатано с оригинала-макета заказчика
в республиканском унитарном предприятии
«Издательский центр Белорусского государственного университета».
Свидетельство о государственной регистрации издателя, изготовителя,
распространителя печатных изданий № 2/63 от 19.03.2014.
Ул. Красноармейская, 6, 220030, Минск.