А.В. БАБАШ

МОНОГРАФИЯ

ДЕШИФРОВАНИЕ КЛАССИЧЕСКИХ ШИФРОВ

Теоретическая и практическая стойкость шифров

Дешифрование шифров тотальным методом

Дешифрование шифров методом эквивалентных ключей

Дешифрование шифров гаммирования

Дешифрование дисковых шифраторов на основе развития атаки «человек посредине»

Дешифрование шифрующих автоматов с помощью их приближенных моделей

КНОРУС

А.В. Бабаш

ДЕШИФРОВАНИЕ КЛАССИЧЕСКИХ ШИФРОВ

Монография

КНОРУС • МОСКВА • 2024

УДК 004.056.55
ББК 32+32.811.4
Б12

Рецензенты:
П.Б. Хорев, Национальный исследовательский университет «МЭИ», канд. техн. наук, доц.,
А.М. Чеповский, Российский университет дружбы народов (РУДН), Высшая школа экономики (НИУ ВШЭ), д-р техн. наук, проф.

Автор
А.В. Бабаш, Российский экономический университет имени Г.В. Плеханова

Бабаш, Александр Владимирович.
Б12 Дешифрование классических шифров : монография / А.В. Бабаш. — Москва : КНОРУС, 2024. — 176 с.

ISBN 978-5-406-11995-2

Большинство разделов написаны в автономном стиле. Для изучения материалов необходимо знать простейшие обозначения математики, в частности простейшие вероятностные понятия и обозначения.

Материал монографии сосредоточен на новых методах дешифрования классических шифров: шифр случайного гаммирования и его частный случай — шифр Вернама; шифр Виженера; шифр простой замены; шифр перестановки; шифр Джефферсона; шифр Тук-тук; шифр IA; дисковые шифраторы, блочные шифры как шифры простой замены с большой мощностью алфавита.

Для студентов специалитета и аспирантов, обучающихся по профилю «Защита информации», а также специалистов по защите информации.

Ключевые слова: шифр случайного гаммирования; шифр простой замены; шифр перестановки; шифр Джефферсона; шифр Тук-тук; дисковые шифраторы; блочные шифры.

УДК 004.056.55
ББК 32+32.811.4

Бабаш Александр Владимирович

ДЕШИФРОВАНИЕ КЛАССИЧЕСКИХ ШИФРОВ

Изд. № 678836. Подписано в печать 13.07.2023. Формат 60×90/16.
Гарнитура «Newton». Печать офсетная.
Усл. печ. л. 11,0. Уч.-изд. л. 10,2.

ООО «Издательство «КноРус».
117218, г. Москва, ул. Кедрова, д. 14, корп. 2.
Тел.: +7 (495) 741-46-28.
E-mail: welcome@knorus.ru www.knorus.ru

ISBN 978-5-406-11995-2

Содержание