М. А. Полтавцева
Д. С. Лаврова

ВЫСОКОПРОИЗВОДИТЕЛЬНЫЕ СИСТЕМЫ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

«Инфра-Инженерия»

М. А. Полтавцева, Д. С. Лаврова

ВЫСОКОПРОИЗВОДИТЕЛЬНЫЕ СИСТЕМЫ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

2-е издание

Рекомендовано Северо-Западным региональным отделением ФУМО по информационной безопасности в качестве учебного пособия для студентов высших учебных заведений, обучающихся по УГСН 10.00.00 «Информационная безопасность» по программам подготовки бакалавров, магистров, специалистов

Москва Вологда
«Инфра-Инженерия»
2023

УДК 004.65
ББК 32.973.2
П52

Рецензенты:
ведущий научный сотрудник СПбФ АО «НПК "ТРИСТАН"»
д. т. н., профессор *Лебедев И. С.*;
зав. кафедрой защищенных систем связи СПбГУТ
к. т. н., доцент *Красов А. В.*

Полтавцева, М. А.

П52 Высокопроизводительные системы обнаружения вторжений : учебное пособие / М. А. Полтавцева, Д. С. Лаврова. – 2-е изд. – Москва ; Вологда : Инфра-Инженерия, 2023. – 152 с. : ил., табл.
ISBN 978-5-9729-1213-1

Рассмотрено построение высокопроизводительных систем обнаружения вторжений в компьютерных сетях и киберфизических системах. Приведены понятие и принципы обработки больших данных, архитектура систем высокой нагрузки, методы предобработки информации при обнаружении вторжений. Рассмотрены различные методы обнаружения вторжений, включая новые подходы на основе технологий искусственного интеллекта.

Для студентов, обучающихся по направлению «Информационная безопасность», и преподавателей, специализирующихся в области информационной безопасности. Может быть полезно широкому кругу специалистов, интересующихся вопросами обнаружения вторжений в системах с большим объемом циркулирующих данных.

УДК 004.65
ББК 32.973.2

ISBN 978-5-9729-1213-1

ОГЛАВЛЕНИЕ