АННОТАЦИЯ

Дипломная работа посвящена теме «Разработка компонента сбора и предварительной обработки данных системы управления информацией и событиями безопасности (SIEM-система)». Дипломная работа состоит из раздела наиболее важных объектов, раздела SIEM-системы, программного раздела, раздела безопасности жизнедеятельности и экономической части.

В данной работе особое внимание было уделено функционалу нормализации и анализу деятельности компонентов SIEM-системы. Были проанализированы и представлены программные решения для службы восстановления данных. Программное решение написано на программном языке Python 3.6. Основной функцией программы является нормалицаия логов из различных источников в один формат. До обработки логов предусматривается отдельное разделение логов на схожие форматы.