Аннотация

В дипломном проекте был реализован программный комплекс, сочетающий в себе модули анализа инцидентов, правил, шифрования, мониторинг и созданием правил кросс-корреляции с использованием SearchInform SIEM (System information and Event Management), Data Center. Основным приоритетом данной системы, является интеграция (внедрение) в ближайшие сроки и отлично подходящей среднего и малого предприятия с повышением уровня безопасности на новый уровень. Совместные модули DLP, DataCenter, Web Analytic, Data Report Center – позволяют обеспечить информационную безопасность во всех уровнях и этапах развития, а простая интеграция позволит моментально соединить источники с SIEM. Web Analytic, Data Report – предоставляют расширенную карту инцидентов и возможных угроз. Расследование инцидентов будет быстрым и оперативным в режиме реального времени, позволяя отсеивать более важные задачи для организации.