





**АНАЛИЗ ВРЕДОНОСНОГО ТРАФИКА И СИСТЕМЫ ДОМЕННЫХ ИМЕН**

Аббасова Т. С.

к.т.н. доцент

Елькин С.В.

Любова А.С.

Гунина Е.В.

бакалавры по направлению подготовки

«Информационные системы и технологии»

Технологический университет («МГОТУ»)

Россия, г. Королев

Проанализированы характеристики системы доменных имен (DNS) и анализ вредоносных программ, каналы DNS, трафик DNS, каналы распределения полезной нагрузки; показано, что вредоносные программы становятся все более опасными с каждым днем.

*Ключевые слова:* DNS сервер, угрозы, Zeus интернет бот, DDoS, кибератака, вредоносная программа, каналы распределения полезной нагрузки.

Серверы команд и управления хостом обычно используются для обнаружения зараженных компьютеров. Основная задача – найти вредоносные программы. Вредоносные программы включают в себя рассылку спама, кражу учетных данных, запуск атак типа «отказ в обслуживании».

Как статический, так и динамический анализ вредоносных программ, а также мониторинг трафика системы доменных имен (DNS) предоставляют ценную информацию о вредоносных действиях и помогают экспертам по безопасности обнаруживать и защищать от многих кибератак [1,2].

Чтобы понять внутреннюю работу наборов инструментов для отражения кибератак, был представлен подробный анализ обратного инжиниринга набора инструментов для борьбы с преступностью Zeus. Анализ позволяет представить структуру сообщений сети бота Zeus. Эта структура может быть использована для извлечения ценных компьютерных данных из анализируемого вредоносного ПО. Полученные сведения помогают раскрыть важные сведения о различных кибератаках и раскрывают домены нарушителей, а также сети вредоносной инфраструктуры.