УДК 004.056

АНАЛИЗ МЕР ЗАЩИТЫ ОТ ТАКТИК КОМПЬЮТЕРНЫХ АТАК С ИСПОЛЬЗОВАНИЕМ СТЕГАНОГРАФИИ

Клишин Д.В. (ИТМО), **Федосенко М.Ю.** (ИТМО), **Агарков А.В.** (ИТМО)
Научный руководитель – кандидат технических наук, доцент Чечулин А.А.
(ИТМО)

Введение. Методы стеганографии используются в таких тактиках компьютерных атак как: доставка вредоносного программного обеспечения, управление вредоносным программным обеспечением, сокрытие действий вредоносного программного обеспечения от обнаружения средствами защиты информации, вывод из информационной инфраструктуры скомпрометированной информации. В зависимости от тактики компьютерной атаки могут применяться следующие основные типы стеганографии [4]: текстовая, в изображении, в звуке, в видео, в метаданных, в сетевых протоколах.

Основная часть. В среде разработчиков вредоносного программного обеспечения отмечен рост использования стеганографии не только для вывода информации из информационной инфраструктуры предприятий и сокрытия коммуникации с командным центром [1], но и для доставки модулей вредоносного программного обеспечения на целевой объект. Сложность обнаружения компьютерных атак с использованием стеганографии по отношению к атакам с использованием криптографии обусловлена тем, что в криптографии известен факт передачи секретного сообщения, но скрыто только его содержание, а в стеганографии не известно о факте передачи секретного сообщения.

С учетом тактик компьютерных атак с использованием стеганографии существуют следующие меры защиты:

1) Выявление аномалий в информационной инфраструктуре с помощью средств защиты информации такого типа как Anti Advanced Persistent Threat.
2) Анализ сетевого трафика с помощью таких решений как Deep Packet Inspection, Intrusion Detection System, Intrusion Prevention System.
3) Защита конечных точек с помощью таких решений как антивирусы и виртуальные песочницы.
4) Контроль действий пользователей с помощью решений таких решений как Data Leak Prevention.
5) Анализ содержимого файлов и обезвреживание вредоносного кода или объектов, содержащихся в них, с помощью решений класса Content Disarm & Reconstruction.
6) Обучение пользователей правилам информационной безопасности.

Выводы. Проведен анализ существующих и перспективных мер защиты [2] [3] от тактик компьютерных атак с использованием стеганографии.

Список использованных источников:

1. MITRE ATT&CK Enterprise: – URL: https://attack.mitre.org/matrices/enterprise/ (дата обращения 02.02.2024).
2. Content Disarm & Reconstruction (CDR) Software: – URL: https://sourceforge.net/software/content-disarm-reconstruction-cdr/ (дата обращения 02.02.2024).
3. Реализация мер по защите информации и обеспечению безопасности из приказов ФСТЭК России: – URL: https://zlonov.ru/measures/ (дата обращения 02.02.2024).
4. М.Ю. Федосенко, С.В. Беззатеев. Анализ проблематики применения методов стеганографии при осуществлении противоправных действий и её роли в цифровой криминалистике.