# МЕРЫ ПРОТИВОДЕЙСТВИЯ ИСПОЛЬЗУЕМЫМ В ХОДЕ ПРОВЕДЕНИЯ КОМПЬЮТЕРНЫХ АТАК СТЕГАНОГРАФИЧЕСКИМ ТЕХНИКАМ

*Анисимов Е. С.[1], Крылов Г. О.[2]*

**DOI:** 10.21681/2311-3456-2025-4-107-116

***Целью работы*** *является определение возможных путей противодействия использованию стеганографических техник при проведении компьютерных атак, включая разработку программного средства стеганографического анализа в качестве примера одного из решений.*

***Метод исследования:*** *анализ основных сценариев применения стеганографии при проведении компьютерных атак; анализ основных методов стеганографического анализа и представленных в открытом доступе тестов безопасности; разработка и программная реализация программного средства стеганографического анализа изображений; экспериментальное исследование и оценка разработанного программного средства.*

***Результат исследования:*** *сформулированы основные направления противодействия стеганографическим техникам проведения компьютерных атак. Разработано программное средство комплексного стеганографического анализа изображений с применением нейронной сети для определения наличия в объекте стеганографической LSB-вставки. Проведена оценка полученных результатов работы модели. Сформулированы направления дальнейших исследований, а также обозначены области практического применения результатов работы, в частности, по совершенствованию SIEM решений и DLP систем.*

***Научная новизна*** *заключается в исследовании противодействия стеганографическим механизмам как техникам проведения компьютерных атак. Также предлагается вариант стеганографического анализа, основанный на комплексном применении нескольких методов анализа.*

***Ключевые слова:*** *стеганография, стеганографический анализ, MITRE ATT&CK, SIEM, DLP, компьютерные атаки, нейронные сети, машинное обучение, Cyber Kill Chain.*

## Введение

Одним из ориентиров для многих средств защиты информации при определении их функциональных возможностей является MITRE ATT&CK – матрица с описанием техник, применяемых нарушителями в рамках компьютерных атак. В данной матрице отдельные техники представлены идентификаторами с описанием их содержания, что дополнено ссылками на информационные материалы с упоминаниями их реального применения атакующими. Таким образом, для некоторой компьютерной атаки допустимо осуществить декомпозицию на отдельные элементы, каждый из которых является определённой техникой из матрицы. Подобное разделение атак на части несколько упрощает задачи противодействия им, поскольку в отношении одной техники проще выделять факторы её обнаружения (обнаружения последствий её использования нарушителями), а также зачастую легче локализовать фрагмент проведения атаки и принять меры противодействия. При общем взгляде на MITRE ATT&CK в контексте некоторого средства защиты информации допустимой является оценка охвата матрицы данным средством с позиции его назначения. Например, для SIEM системы охват отдельной техники из MITRE ATT&CK означает наличие у решения возможности обнаружить в сети организации активность атакующих, придерживающихся в составе атаки данной техники.

В связи с этим один из возможных путей совершенствования средств защиты информации – их дополнение с целью увеличения покрытия техник MITRE ATT&CK. То есть для некоторого существующего средства проводится оценка его текущих функциональных возможностей, которые соотносятся с техниками MITRE ATT&CK, после чего особое внимание обращается на не входящие в область покрытия техники. В отношении данных техник определяются инструменты их идентификации или противодействия, на основании чего проводится работа по улучшению средства защиты информации.

Ранее в работе [2] отмечалась присутствующая у нарушителей возможность применения стеганографических методов для организации скрытых коммуникаций в рамках проводимых компьютерных атак. Такая возможность представляет особый интерес

1 Анисимов Ефим Сергеевич, магистр, Финансовый университет при Правительстве Российской Федерации, Москва, Россия. E-mail: EAnisimov_Sci@mail.ru, ORCID: 0000-0002-2632-4439.

2 Крылов Григорий Олегович, доктор физико-математических наук, профессор, Военный университет им. кн. Александра Невского Министерства обороны Российской Федерации, Национальный исследовательский ядерный университет «МИФИ», Финансовый университет при Правительстве Российской Федерации, Москва, Россия. E-mail: op50@mail.ru, ORCID: 0000-0001-8145-1994.

по причине высокой сложности идентификации соответствующей злонамеренной активности нарушителей в сети организации, осуществляемой подобным образом. Для описания данных действий сообществом введены идентификаторы T1001.002, T1027.003, T1406.001 в составе техник нарушителей из матрицы MITRE ATT&CK. Обзор некоторых российских средств защиты информации в части покрытия ими матрицы MITRE ATT&CK показал преобладающее отсутствие реализаций, позволяющих полностью покрыть отмеченные «стеганографические» техники: в лучших случаях найдены примеры охвата только техники T1027.003. Данное наблюдение подтверждает актуальность исследования вопросов обнаружения и противодействия использованию нарушителями стеганографии для различных действий. Другая работа [1] также содержит обзор применений стеганографии как элемента компьютерных атак. Соответственно, в рамках настоящей работы авторами преследуется цель оценки использования нарушителями отмеченных техник компьютерных атак и определения возможных мер противодействия.

### Стеганографические механизмы как элемент компьютерных атак

Прежде проведём оценку потенциала применения стеганографических алгоритмов для достижения различных целей атакующих. Если рассматривать компьютерные атаки в разрезе известной семиэтапной модели Cyber Kill Chain проведения атак, то основные шаги нарушителей, на которых имеется некоторый обмен информацией между сетью атакуемого объекта и внешним миром:

- доставка вредоносного программного обеспечения – 3 этап;
- организация канала связи и установление соединения с командно-управляющим Сервером (Command and Control, C2 Сервер) – 6 этап;
- осуществление целевых действий (создание утечки защищаемой информации и пр.) – 7 этап.

Соответственно, стоит оценить: возможно ли применять стеганографию для выполнения отмеченных мероприятий в составе атаки. Обзор источников показал, что нарушители действительно применяют стеганографические методы для реализации обозначенных элементов атак.

Например, источники [5, 12, *Staged Malware*[3]] содержат примеры или описание инструментов сокрытия некоторого вредоносного материала в контейнерах-изображениях посредством таких стеганографических методов, как LSB и сокрытие с помощью LSB в коэффициентах DCT (дискретного косинусного преобразования). Данные примеры также доказывают наличие возможности использования стеганографии в целях доставки вредоносного программного обеспечения.

Таким образом, показано наличие возможностей использования стеганографических методов в рамках проведения компьютерных атак. Данные возможности подтверждаются и реальными примерами, составленными специалистами по результатам расследований произошедших атак. Перечислим несколько из подобных примеров в качестве подтверждения представленного тезиса:

- обзор методов работы APT-группировки (APT – Advanced Persistent Threat, целевая продолжительная атака повышенной сложности) Turla показал[4], что потенциальный арсенал для их функционирования включает, среди прочего, техники MITRE ATT&CK T1001.002 и T1027.003;
- атака группировки MuddyWater содержала[5] действия по использованию техники T1027.003: нарушители скрывали обфусцированный исходный код на JavaScript в медиа-файле temp.jpg;
- серия атак с использованием трояна Necro.N, в рамках которых применялись[6] стеганографические механизмы для сокрытия вредоносной нагрузки в изображениях (специалистами соотносится с техникой T1406.001) для осуществления её загрузки с C2 Сервера на заражённое устройство.

В дополнение, без взаимосвязи с реальными случаями данный факт возможности использования стеганографии в рамках компьютерных атак косвенно был подтверждён выше посредством обозначения соответствующих техник в матрице MITRE ATT&CK, которые, в свою очередь, не формализуются и не вносятся в матрицу без веских оснований существования.

### Основные подходы противодействия стеганографическим техникам

Представим возможные пути противодействия нарушителям, действующим в обозначенных формах. Основных подходов к решению такой проблемы можно выделить два:

Использование средств комплексного стеганографического анализа, которые будут применяться для

3 Steganography based Staged Malware 001. [Электронный ресурс] URL: https://github.com/Shauryae1337/Steganography-based-Staged-Malware. (дата обращения: 18.04.2025).

4 LunarWeb and LunarMail: The Secret Weapons of the Turla APT. Hiveforce Labs. [Электронный ресурс] URL: https://www.hivepro.com/wp-content/uploads/2024/05/LunarWeb-and-LunarMail-The-Secret-Weapons-of-the-Turla-APT_TA2024191.pdf. (дата обращения: 21.04.2025).

5 Iranian Government-Sponsored Actors Conduct Cyber Operations Against Global Government and Commercial Networks. CISA. [Электронный ресурс] URL:https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-055a. (дата обращения: 21.04.2025).

6 The Mobile Malware Chronicles: Necro.N – Volume 101. Zimperium. [Электронный ресурс] URL: https://zimperium.com/blog/the-necro-n-chronicles-volume-101. (дата обращения: 21.04.2025).

анализа передаваемых файлов на предмет оценки возможного наличия в них стеганографической вставки;

Настройка системы защиты объекта по результатам учений информационной безопасности на основе проведения различных тестов, имитирующих реализацию интересующих с позиции противодействия им техник атакующих (совершенствование системы защиты на основе взаимодействия Red и Blue Team).

### Средство стеганографического анализа

Относительно применения средств стеганографического анализа стоит отметить, что они не являются универсальным и безошибочным решением проблемы применения стеганографии в рамках компьютерных атак. Однако их и нельзя игнорировать, напротив, они представляют собой практически полезное дополнение функционирующих на объекте защиты средств в составе систем обеспечения информационной безопасности (в особенности систем предотвращения утечек – DLP-систем – и SIEM решений). Авторами в контексте исследования вопроса противодействия использованию стеганографических методов при проведении компьютерных атак было разработано программное средство, которое предназначено для проведения комплексного стеганографического анализа медиа-файлов с целью идентификации наличия в них стеганографической вставки или её отсутствия. Представим описание структуры данного программного обеспечения с приведением краткой характеристики основных достигнутых параметров работы.

Специалистами разработано множество различных методов стеганографического анализа, и данное направление продолжает развиваться, в частности, с уделением особого внимания применению моделей машинного обучения для данных задач. Подобная тенденция в развитии стеганографического анализа обусловлена среди прочего и тем, что нарушители в последнее время активно используют генеративные модели для сокрытия некоторой вставки в не готовых изображениях, а в генерируемом контейнере. Разработки подобных методов описаны, например, в работах [6, 13]. Подобные изменения требуют более активного развития направлений стеганографического анализа, в особенности с применением искусственного интеллекта. В свою очередь, ряд специалистов отмечает, что научное сообщество стеганографическому анализу уделяет меньшее внимание нежели стеганографическим методам сокрытия [7].

Авторами при создании средства стеганографического анализа была сформирована гипотеза о предпочтительности совместного применения нескольких методов стеганографического анализа с точки зрения повышения точности определения вероятного наличия стеганографической вставки в исследуемом объекте. В связи с этим, учитывая широкое использование метода LSB (Least Significant Bit – стеганографический метод сокрытия данных в младших значащих битах), был проведён обзор основных методов стеганографического анализа изображений на предмет обнаружения в них вставок, осуществлённых именно методом LSB. По итогам анализа содержания источников [3, 8, 9, 10] в качестве основных методов для дальнейшей реализации были выбраны следующие:

- регулярный-сингулярный анализ (Regular or Singular, RS-анализ);
- метод анализа подобия значений пискелей (Pixel Similarity Weights — PSW);
- метод хи-квадрат на основе статистического анализа пар значений.

Отметим ключевые особенности указанных методов стеганографического анализа.

RS-анализ строится на функции гладкости (регулярности) и функции флиппинга. Функция регулярности $f$ однозначно неопределена в рамках метода: она может быть дисперсией значений внутри данного блока изображения (анализируемое изображение разбивается на квадратные блоки $G$: $nxn$) или суммой разностей значений пикселей (1):

$$f(G) = \sum_{i=1}^{n-1} |x_{i+1} - x_i|. \quad (1)$$

Флиппинг-функция должна обладать свойством $F(F(x)) = x$, то есть она инволютивна. Основными вариантами функции флиппинга для изображений являются функция инверсии младшего бита значения пикселя $(F_1)$ и такая же инверсия, только с переносом в старший бит $(F_{-1})$:

$$F_1 = 0 - 1;\ 2-3;\ 4-5;\ \ldots;\ 252-253;\ 254-255,$$
$$F_{-1} = 1 - 2;\ 3-4;\ 5-6;\ \ldots;\ 253-254;\ 255-0.$$

Соответственно, применение к отдельному блоку изображения функции гладкости и флиппинг-функции даст различные результаты, что ложится в основу RS-стеганоанализа. Определённое соотношение результатов функций от данного блока позволяет различать три класса блоков:

- неиспользуемые группы $U$: это блоки $G \in U \iff$ $\iff f(F(G)) = f(G)$;
- регулярные группы $R$: блоки $G \in R \iff f(F(G)) =$ $= f(G)$;
- сингулярные группы $S$: блоки $G \in S \iff f(F(G)) =$ $= f(G)$.

В рамках RS стеганографического анализа аналитик обращает внимание на количество блоков, которые попали в группы $R$ и $S$, причём отдельно

рассчитывается такое значение для флиппинг-функции $F_1$ и отдельно для $F_{-1}$. Соответственно, такие количества блоков в группах при разных флиппинг-функциях можно обозначить как $R_{cnt}$ и $S_{cnt}$, $R_{-cnt}$ и $S_{-cnt}$.

RS-метод стеганографического анализа основывается на предположении пренебрежимо малых отличий между количествами блоков в сингулярной и регулярной группах независимо от применённой при расчётах флиппинг-функции в случае «чистого», обычного изображения, то есть: $R_{cnt} \approx R_{-cnt}$ и $S_{cnt} \approx S_{-cnt}$.

Если же для анализируемого изображения данное соотношение не выполняется, использование другой флиппинг-функции вносит значительное расхождение в количество блоков в соответствующих группах, то делается вывод о высокой вероятности факта проведения над изображением стеганографического преобразования методом LSB.

Дополнительно скажем, что RS-метод стеганографического анализа может иметь дополнения и расширения, в частности, с его помощью можно проводить оценки длины стеганографической вставки.

Метод анализа PSW — это пример метода статистического стеганографического анализа, в основе которого лежит вычисление определённым образом доли идентичных пикселей рассматриваемому. Для рассматриваемого пикселя окружающие пиксели, размещённые в соответствующем квадрате, расположенном от текущего пикселя не дальше, чем на 3 (в некоторых работах предлагается до 4 — глубина анализа строго не ограничивается, однако следует соблюдать баланс между объёмом анализа и вычислительной нагрузкой метода), выделяются окружающие его кольца. То есть для рассматриваемого пикселя с координатами $(i_0,j_0)$ в группу пикселей $Z_d$, где $d \leq 3$, попадут все пиксели с координатами $(i,j): max(|i - i_0|,|j - j_0|) \leq d$. Таким образом, если анализируемый пиксель расположен не вблизи границ изображения, то область $Z_1$ будет содержать 8 пикселей, область $Z_2$ – 16 и $Z_3$ – 24. Наглядно идея такого разделения областей близких пикселей показана на рисунке 1.

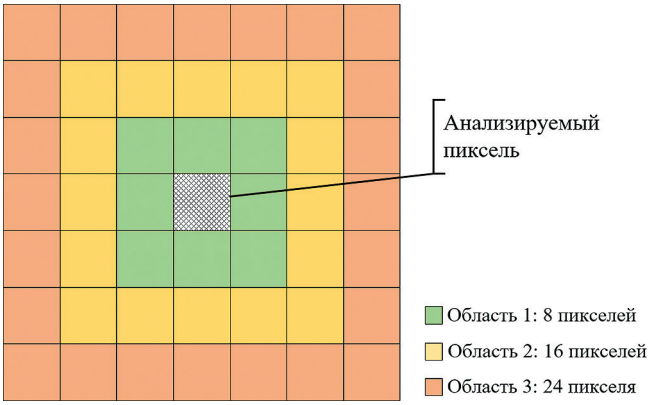


*Рис. 1. Области близких пикселей для определения доли идентичных анализируемому пикселей в рамках метода PSW (Источник: составлено автором по материалам[7])*

В каждой из таких соседствующих зон подсчитывается количество одинаковых с рассматриваемым пикселей. В соответствии с обозначенной идеей обработки изображения формируются наборы значений для дальнейшего анализа, которые образуют основу для второй и не менее важной части метода стеганографического анализа PSW — метода опорных векторов (Support Vector Machine — SVM). SVM – это алгоритм машинного обучения для решения задач классификации/регрессии. В рамках второй части метода первостепенное значение имеет качественная подготовка обучающих выборок для модели. При хорошем подборе примеров изображений, охватывающих как можно большее число сценариев размещения стеганографической вставки и различных изображений без вставки с соответствующими значениями целевой переменной, такая задача классификации посредством SVM решается достаточно хорошо. Таким образом, метод стеганографического анализа PSW предполагает не только статистический анализ изображений на предмет наличия в них скрытых данных, но и машинное обучение, основывающееся на предварительном анализе. Данный подход даёт большую гибкость и адаптивность метода к различным стеганографическим техникам изначального сокрытия данных в контейнере-изображении.

Рассматривая классический подход LSB, предполагающий изменение только одного, самого младшего бита, можно обратить внимание, что преобразование значений байта соответствующего цветового канала происходит в рамках ограниченного набора пар. Например, из значения $(27)_{10} = (11011)_2$ метод LSB может получить значения $(27)_{10} = (11011)_2$ или $(26)_{10} = (11010)_2$ — других возможных результатов по итогам корректировки наименьшего значащего бита нет. В связи с этим заранее возможно обозначить пары значений пикселей, которые имеют место в рамках LSB преобразования, визуально идея таких пар представлена на рисунке 2.

Соответственно, всего имеется 128 пар значений представленного вида (можно также сказать, что число 128 соответствует количеству компонент сильной связности ориентированного графа, в котором 256 вершин, соответствующих значениям от 0 до 255 включительно; а дуги – отражают возможные результаты изменения наименьшего значащего бита). Данное наблюдение (PoV – Pairs of pixel

7 Chaeikar S., Zamani M., Manaf A. B., Zeki A. M. PSW statistical LSB image steganalysis // Multimedia Tools and Applications. 2018. № 77. pp. 805–835. https://doi.org/10.1007/s11042-016-4273-6.

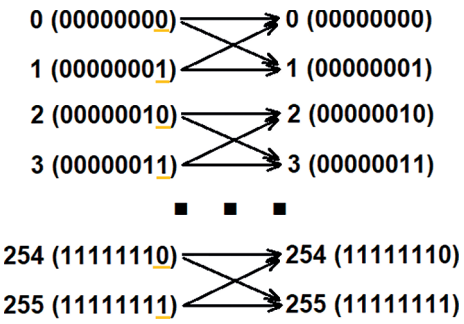


*Рис. 2. Возможные пары-изменения значений пикселей в LSB*

Values) используется в рамках метода хи-квадрат. Для каждой из 128 пар можно подсчитать количество пикселей, соответствующих конкретной паре. Более формально такое количество $c_p$ для пары $(2p, 2p+1)$, где $p \in [0,1,...,127]$ определяется формулой (2):

$$c_p = \frac{|pixel_{value} \in [2p, 2p+1]|}{2}. \quad (2)$$

Для целей метода стеганографического анализа применяются метрики хи-квадрат, а именно подсчитывает хи-квадрат с $p-1$ степенями свободы (3):

$$\chi^2_{p-1} = \sum_{i=1}^{p} \frac{(c_i - c_i^*)^2}{c_i^*}. \quad (3)$$

Теперь готовы все значения для расчёта вероятности $P$ наличия скрытой вставки (4):

$$P = 1 - \frac{1}{2^{\frac{p-1}{2}}\Gamma\frac{p-1}{2}} \int_0^{\chi^2_{(p-1)}} e^{x/2}\, x^{\frac{p-1}{2}-1}\, dx. \quad (4)$$

От полученной вероятности отталкиваются вердикты данного хи-квадрат метода стеганографического анализа.

В соответствии с содержанием методов была осуществлена их программная реализация на языке программирования Python. Каждый из методов составил основу отдельных модулей программного средства, возвращаемым значением которых является некоторое значение вероятности наличия в переданном на анализ в метод изображении LSB-вставки. По предположению, объект анализируется каждым из трёх методов, в результате чего формируется вектор из трёх значений, который служит для формирования матрицы признаков, соответствующей используемому датасету из изображений. По готовности такой матрицы из трёх признаков и соответствующего ей вектора со значениями целевой переменной (0 – стеганографическая вставка отсутствует, 1 – имеется LSB вставка) имеется датасет для обучения и тестирования нейронной сети (для реализации выбрана из пакета Keras). Данный подход к построению программного средства определил его архитектуру, в общем виде которая показана на рисунке 3.

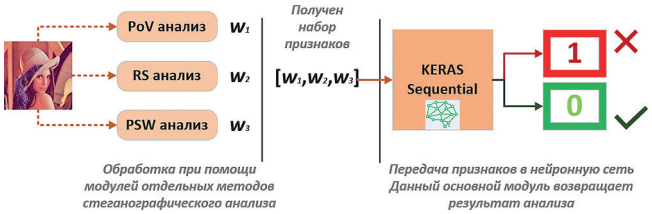


*Рис. 3. Архитектура разработанного программного средства*

Исходный датасет изображений, использованный для подготовки описанной матрицы признаков с результатами стеганографического анализа каждым из методов в отдельности, выбран из источника[8]. Описание данного датасета представлено далее по тексту в таблице 3. По результатам его обработки реализованными модулями PoV (метод хи-квадрат), RS и PSW анализа получена матрица размерности 10000x3 вместе с вектор-столбцом значений булевой целевой переменной. В целом, полученные элементы матрицы содержат подтверждения гипотезы о возможности различных результатов стеганографического анализа одного объекта разными методами. Вычисленные значения свидетельствуют об этом, в связи с чем потенциально возможно достижение синергетического эффекта в сценарии совместного применения различных методов. По причине необходимости получения однозначного результата для отдельного изображения имеющиеся три соответствующих значения-признака определённым образом требовалось свернуть в булево значение целевой переменной. Для этих целей выбрана нейронная сеть с последовательным расположением слоёв из пакета Keras (Keras Sequential). Конечно, пересчёт можно было сделать математически на основе введения коэффициентов и расчёта интегрального показателя, однако при выборе финальной основной модели авторами принималась во внимание возможность дальнейшего её масштабирования (в том числе посредством добавления других методов стеганографического анализа), для чего более применимы нейросетевые решения.

Прокомментируем достигнутые результаты созданного программного средства. До момента окончательного выбора моделей из пакета Keras в качестве основного решения проводилось их сравнение с наиболее сильными представителями не-нейросетевых решений, а именно LightGBM и XGBoost – модели градиентного бустинга над решающими деревьями. В таблице 1 содержатся значения метрик Precision и F1, полученные по результатам тестирования каждой из сравниваемых моделей на тестовой выборке после их обучения.

8 Stego-Images-Dataset. Kaggle. [Электронный ресурс] URL: https://www.kaggle.com/datasets/marcozuppelli/stegoimagesdataset. (дата обращения: 21.04.2025).

*Таблица 1.*

*Показатели работы основного модуля, формирующего результат комплексного стеганографического анализа изображения*

| Модель | Время обучения, с | Время теста, с | Точность (precision) | F1 мера |
|---|---|---|---|---|
| LightGBM | 0,053773 | 0,006964 | 0,676190 | 0,633333 |
| XGBoost | 0,065580 | 0,004790 | 0,676190 | 0,633333 |
| Keras Sequential | 73,067876 | 0,365499 | 0,762100 | 0,686217 |

Представленные значения дают подтверждение предпочтительности выбора нейросетевых решений в качестве основного модуля программного средства, возвращающего некоторое интегральное значение стеганографического анализа на основе результатов отдельных методов, причём не только в качестве отвечающих задачам возможного масштабирования модели, но и по достигнутым в ходе работы показателям.

Приведённое описание позволяет зафиксировать несколько основных выводов о результатах разработки программного средства комплексного стеганографического анализа. Начальная созданная модель характеризуется относительно позитивными результатами работы. Показатель Precision на уровне 76,21% для исследуемой нетривиальной задачи идентификации в анализируемом изображении стеганографической LSB-вставки является весьма хорошим.

*Таблица 2.*

*Существующие тесты безопасности для имитации элементов компьютерных атак с использованием стеганографических методов*

| Техника | Источники тестов безопасности и описание |
|---|---|
| T1001.002 | Тест[9] имитирует сокрытие tar архива в изображении.<br>Тест[10] имитирует сокрытие в изображении скрипта PowerShell с помощью стеганографических методов.<br>Тест[11] имитирует исполнение встроенного в изображение (при помощи стеганографии) Shell скрипта с предварительным его кодированием в BASE64. |
| T1027.003 | Точечный тест[12], его можно считать примером сигнатурного стеганографического анализа, который направлен на обнаружение применения программного обеспечения steghide для сокрытия информации. Авторами данный тест аудита отмечен как соответствующий технике атаки T1027.003, однако область применения представляется практически более широкой, относящийся в то же время и к двум другим рассматриваемым стеганографическим техникам.<br>[11] В данной научной статье авторами также проведена работа, идейно близкая к сигнатурному стеганографическому анализу. Данные материалы не являются тестом, готовым к прямому применению в практических системах, но в то же время представленные в работе результаты формируют ориентир для элементов объектов проверки, на которые следует обращать внимание при анализе. Хотя данное исследование и проводилось применительно к задачам компьютерной криминалистики (форензики), его материалы представляют практическую значимость для задач стеганографического анализа в ходе процессов обнаружения и противодействия компьютерным атакам. |
| T1406.001 | Не найдены тесты безопасности, предназначенные для отработки техники матрицы MITRE ATT&CK с явно указанным идентификатором. |

9 T1001.002 – Data Obfuscation via Steganography. Atomic Test #1 – Steganographic Tarball Embedding. Atomic Red Team. [Электронный ресурс] URL: https://www.atomicredteam.io/atomic-red-team/atomics/T1001.002#atomic-test-1---steganographic-tarball-embedding (дата обращения: 21.04.2025).

10 T1001.002 – Data Obfuscation via Steganography. Atomic Test #2 – Embedded Script in Image Execution via Extract-Invoke-PSImage. Atomic Red Team. [Электронный ресурс] URL: https://www.atomicredteam.io/atomic-red-team/atomics/T1001.002#atomic-test-2---embedded-script-in-image-execution-via-extract-invoke-psimage (дата обращения: 21.04.2025).

11 T1001.002 – Data Obfuscation via Steganography. Atomic Test #3 – Execute Embedded Script in Image via Steganography. Atomic Red Team. [Электронный ресурс] URL: https://www.atomicredteam.io/atomic-red-team/atomics/T1001.002#atomic-test-3---execute-embedded-script-in-image-via-steganography (дата обращения: 21.04.2025).

12 Sigma – Generic Signature Format for SIEM Systems. lnx_auditd_steghide_embed_steganography.yml. [Электронный ресурс. (дата обращения: 21.04.2025).] URL: https://github.com/SigmaHQ/sigma/blob/master/rules/linux/auditd/lnx_auditd_steghide_embed_steganography.yml

### Применение тестов безопасности

По направлению организации проведения тестов безопасности, имитирующих конкретные техники атакующих, стоит отметить наличие примеров конкретных тестов безопасности, которые подготовлены различными крупными командами. В таблице 2 собраны ссылки на тесты безопасности, которые могут использоваться Red Team организации для имитации соответствующих «стеганографических» техник из матрицы MITRE ATT&CK.

Результаты обзора источников различных категорий свидетельствуют о недостаточном охвате различных сценариев применения рассматриваемых стеганографических техник MITRE ATT&CK. В этой связи видится практически полезным накопление материалов, а также в целом использование готовых датасетов для формирования разнообразных примеров медиа-файлов, которые будут в таком случае являться подобным тестом безопасности. Решением для обработки этих материалов может являться модуль в виде модели машинного обучения или нейронной сети, который будет обучаться на подготовленных материалах, результатом же такого обучения являются обновления моделей, способные учитывать ситуации, аналогичные проведённым тестам.

Примерами доступных в открытом доступе датасетов подобного рода, подходящих для тестов, соответствующих названным в настоящей работе техникам матрицы MITRE ATT&CK с основой в виде стеганографических методов, являются следующие наборы данных, собранные в виде таблицы 3.

Выше представлен, конечно, не исчерпывающий перечень допускающих использование для целей настроек моделей датасетов, однако достаточный для получения начального материала работы по рассматриваемому направлению. В то же время не стоит забывать о возможности самостоятельной подготовки обучающих материалов аналогичного

*Таблица 3.*

*Материалы для обучения моделей, предназначенных для идентификации медиа-файлов, содержащих стеганографическую вставку*

| Наименование | Описание датасета |
|---|---|
| Stego-Images-Dataset. N. Cassavia, L. Caviglione, M. Guarascio, G. Manco, M. Zuppelli | Содержит 44000 изображений, содержащих стеганографические вставки (по содержанию: ссылки URL, вредоносный исходный код, адреса контрактов блокчейн-платформы Ethereum и прочие), осуществлённые при помощи алгоритма LSB[13]. |
| JPEG StegoChecker dataset. Mikołaj Płachta, Marek Krzemień, Krzysztof Szczypiorski, Artur Janicki. | Содержит 10000 чёрно-белых изображений, содержащих стеганографические вставки случайного содержания, осуществлённые при помощи алгоритмов J-Uniward, nsF5 и UERD[14]. |
| Stego-Favicons-Dataset. M. Guarascio, M. Zuppelli, N. Cassavia, L. Caviglione, G. Manco. | Репозиторий состоит из двух датасетов:<br>– первый содержит 360000 изображений, из которых 60000 – исходные изображения без вставок, 60000 – изображения со стеганографическими вставками вредоносного PHP кода, 240000 изображений со стеганографическими вставками URL;<br>– второй содержит 90000 изображений, из которых 15000 – чистые исходные изображения, 15000 – изображения со стеганографическими вставками PHP кода в формате BASE64, 60000 – изображения со стеганографическими вставками URL.<br>Стеганографические вставки сделаны при помощи стеганографического алгоритма LSB[15]. |
| Прочие датасеты | Собрание ссылок на прочие датасеты также составлены в работах других авторов, например, примеры имеются в статье [4] |

13 Stego-Images-Dataset. Kaggle. [Электронный ресурс (дата обращения: 21.04.2025).] URL: https://www.kaggle.com/datasets/marcozuppelli/stegoimagesdataset (дата обращения: 21.04.2025).

14 JPEG StegoChecker dataset. Kaggle. [Электронный ресурс (дата обращения: 21.04.2025)] URL: https://www.kaggle.com/datasets/h2020simargl/jpeg-stegochecker-dataset?select=gfr_cover.csv

15 Stego-Favicons-Dataset. GitHub. [Электронный ресурс] URL: https://github.com/Ocram95/Stego-Favicons-Dataset (дата обращения: 21.04.2025).

характера, которые в зависимости от постановки задач могут и превосходить указанные по вкладу, вносимому в конечное качество работы моделей. Например, улучшение может заключаться в использовании различных стеганографических алгоритмов для сокрытия вставок; формировании пула разнообразных по содержанию и характеристикам изображений, используемых в качестве контейнера, а также составлении наборов вставок вариативного содержания.

## Заключение

В рамках настоящей статьи отмечена актуальность совершенствования систем обеспечения информационной безопасности в направлении учёта ими угроз, связанных с применением стеганографических методов сокрытия информации. Подобные техники имеют собственные идентификаторы в матрице MITRE ATT&CK, и они могут быть использованы для различных действий, в частности, для доставки вредоносного программного обеспечения, осуществления взаимодействия с C2 Сервером, выполнения целевых действий, организации утечки защищаемой информации. Латентная природа действий по передаче данных стеганографическими методами служит хорошим мотивом для взятия таких техник на вооружение нарушителями, поэтому осуществление указанного круга действий является актуальной угрозой, связанный с реализацией которой риск требует определённой обработки.

Теоретическая значимость работы заключается в исследовании направления стеганографического анализа, в отношении которого отмечают меньшее внимание со стороны сообщества. Полученные результаты вносят вклад и в прикладную науку, состоящий в определении возможностей противодействия стеганографическим техникам, применяемым при проведении компьютерных атак.

Исследование отражает несколько возможных путей противодействия стеганографическим техникам: проведение стеганографического анализа файлов и моделирование действий нарушителей, применяющих подобные техники, на основе которого проводится донастройка средств защиты информации, по итогам чего допустима отработка основных сценариев активности нарушителей, включённых в использованные тесты безопасности.

В рамках первой группы мер приведён пример разработки программного средства стеганографического анализа с обзором результатов его работы.

В части проведения тестов безопасности в работе авторами собраны примеры ссылок на применимые для этого материалы. Отметим, что в открытом доступе представлено незначительное количество тестов рассматриваемого класса, поэтому в этой части оптимальной может стать собственная подготовка материалов.

По мнению авторов, предложенные направления мер защиты и, в особенности, разработанное в рамках исследования программное средство стеганографического анализа имеют возможность получить практическое применение в рамках совершенствования как систем обеспечения информационной безопасности организаций в целом, так и применительно к улучшению отдельных классов средств защиты информации, среди которых в данном случае основными являются DLP решения и SIEM системы. Упомянем, что обзор возможностей ряда ведущих российских SIEM решений в контексте охвата ими техник матрицы MITRE ATT&CK отразил неполное покрытие ими рассматриваемых в настоящем исследовании техник T1001.002, T1027.003, T1406.001, что одновременно дополнительно подтверждает актуальность вопроса и служит подтверждением потенциала практической применимости полученных результатов. В свою очередь, положительный вклад в развитие обозначенных классов средств защиты информации, которые занимают далеко не последнее место в структуре продуктов сферы, будет способствовать улучшению состояния информационной безопасности Российской Федерации.

**Литература**


1. Клишин Д. В., Федосенко М. Ю. Применение стеганографии при осуществлении компьютерных атак на информационную инфраструктуру предприятий // Экономика и качество систем связи. 2024. № 2(32). с. 158–166.
2. Ревенков П. В., Анисимов Е. С. Утечка информации: классификация каналов и влияние на типичные банковские риски // В центре экономики. 2025. № 1. Т. 6. с. 1–6.
3. Apau R., Hayfron-Acquah J. B., Asante M., Twum F. A multilayered secure image steganography technique for resisting regular-singular steganalysis attacks using elliptic curve cryptography and genetic algorithm // International conference on ICT for sustainable development. Singapore: Springer Nature Singapore, 2023. с. 427–439. https://doi.org/10.1371/journal.pone.0308807.
4. Badar L. T., Carminati B., Ferrari E. A comprehensive survey on stegomalware detection in digital media, research challenges and future directions // Signal Processing. 2025. С. 109888. https://doi.org/10.1016/j.sigpro.2025.109888.
5. Chaganti R., Ravi V., Alazab M., Pham T. D. Stegomalware: A Systematic Survey of MalwareHiding and Detection in Images, Machine LearningModels and Research Challenges // arXiv preprint arXiv:2110.02504. 2021. https://doi.org/10.48550/arXiv.2110.02504.
6. Huo L., Chen R., Wei J., Huang L. A high-capacity and high-security image steganography network based on chaotic mapping and generative adversarial networks // Applied Sciences. 2024. 14 (3). с. 1225. https://doi.org/10.3390/app14031225.
7. Kombrink M. H., Geradts Z. J. M. H., Worring M. Image steganography approaches and their detection strategies: A survey // ACM Computing Surveys. 2024. № 57 (2). с. 1–40. https://doi.org/10.1145/3694965.

8. Lin W. B., Lai T. H., Chou C. L. Chi-square-based steganalysis method against modified pixel-value differencing steganography // Arabian Journal for Science and Engineering. 2021. Т. 46. №. 9. с. 8525–8533. https://doi.org/10.1007/s13369-021-05554-2.
9. Shankar D. D., Azhakath A. S. Random embedded calibrated statistical blind steganalysis using cross validated support vector machine and support vector machine with particle swarm optimization // Scientific Reports. 2023. № 13(1). с. 2359. https://doi.org/10.1038/s41598-023-29453-8.
10. Shehab D. A., Alhaddad M. J. Comprehensive survey of multimedia steganalysis: Techniques, evaluations, and trends in future research // Symmetry. 2022. № 14(1). с. 117. https://doi.org/10.3390/sym14010117.
11. Stefan Kiltz, Jana Dittmann, Fabian Loewe, Christian Heidecke, Max John, Jonas Mädel and Fabian Preißler. 2024. Forensic Image Trace Map for Image-Stego-Malware Analysis: Validation of the Effectiveness with Structured Image Sets. In Proceedings of 2024 ACM 12th ACM Workshop on Information Hiding and Multimedia Security (ACM IH&MMSEC'24), June 24–26, 2024, Baiona, Spain. ACM, New York, NY, USA, с. 6. https://doi.org/10.1145/3658664.3659659.
12. Strachanski F., Petrov D., Schmidbauer T., Wendzel S. A Comprehensive Pattern-based Overview of Stegomalware // Proceedings of the 19th International Conference on Availability, Reliability and Security. 2024. с. 1–10. https://doi.org/10.1145/3664476.3670886.
13. Volkhonskiy D., Nazarov I., Burnaev E. Steganographic generative adversarial networks // Twelfth international conference on machine vision (ICMV 2019). SPIE, 2020. Т. 11433. с. 991–1005. https://doi.org/10.48550/arXiv.1703.05502.

# COUNTERMEASURES APPLICABLE FOR CYBERATTACK STEGANOGRAPHIC TECHNIQUES

*Anisimov E.S.[16], Krylov G. O.[17]*

***Keywords:*** *steganography, steganalysis, MITRE ATT&CK, SIEM, DLP, cyberattack, neural networks, machine learning, Cyber Kill Chain.*

***The purpose of the article*** *is defining of main countermeasures for steganographic techniques usage in cyberattacks, comprising the development of a steganalysis tool as an example of one of the ways.*

***Research methods:*** *steganography in cyberattacks usage scenario analysis; steganalysis methods and available security tests review; image steganalysis software tool development; experimental evaluation of the developed tool.*

***The result obtained:*** *main directions of countermeasures for cyberattack steganographic techniques were formulated in the article. Image complex steganalysis software tool using a neural network to LSB insertion detection in an object has been developed. The results of the developed tool were evaluated. The study reveals directions for further researches and main applications of the study's results, in particular, for improving DLP and SIEM solutions.*

*The scientific novelty of the article is countermeasures for steganographic mechanisms as cyberattack techniques research. In the article proposed a steganalysis scenario based on several analysis methods combined usage.*

## References

1. Klishin D., Fedosenko M. The use of steganography in the implementation of computer attacks on the information infrastructure of enterprises. Economy and quality of communication systems. 2024; 2 (32). pp. 158–166.
2. Revenkov P. V., Anisimov E. S. Information Leak: Classification of Channels and Impact on Typical Banking Risks. In the Center of Economy. 2025; 1 (6). pp. 1–6.
3. Apau R., Hayfron-Acquah J. B., Asante M., Twum F. A multilayered secure image steganography technique for resisting regular-singular steganalysis attacks using elliptic curve cryptography and genetic algorithm // International conference on ICT for sustainable development. Singapore: Springer Nature Singapore, 2023. pp. 427–439. https://doi.org/10.1371/journal.pone.0308807.
4. Badar L. T., Carminati B., Ferrari E. A comprehensive survey on stegomalware detection in digital media, research challenges and future directions // Signal Processing. 2025. p. 109888. https://doi.org/10.1016/j.sigpro.2025.109888.
5. Chaganti R., Ravi V., Alazab M., Pham T. D. Stegomalware: A Systematic Survey of MalwareHiding and Detection in Images, Machine LearningModels and Research Challenges // arXiv preprint arXiv:2110.02504. 2021. https://doi.org/10.48550/arXiv.2110.02504.
6. Huo L., Chen R., Wei J., Huang L. A high-capacity and high-security image steganography network based on chaotic mapping and generative adversarial networks // Applied Sciences. 2024. 14(3). p. 1225. https://doi.org/10.3390/app14031225.
7. Kombrink M. H., Geradts Z. J. M. H., Worring M. Image steganography approaches and their detection strategies: A survey // ACM Computing Surveys. 2024. № 57(2). pp. 1–40. https://doi.org/10.1145/3694965.
8. Lin W. B., Lai T. H., Chou C. L. Chi-square-based steganalysis method against modified pixel-value differencing steganography // Arabian Journal for Science and Engineering. 2021. V. 46. №. 9. pp. 8525–8533. https://doi.org/10.1007/s13369-021-05554-2.
9. Shankar D. D., Azhakath A. S. Random embedded calibrated statistical blind steganalysis using cross validated support vector machine and support vector machine with particle swarm optimization // Scientific Reports. 2023. 13 (1). pp. 2359. https://doi.org/10.1038/s41598-023-29453-8.

16 Efim S. Anisimov, master's degree, Financial University under the Government of the Russian Federation, Moscow, Russia. E-mail: EAnisimov_Sci@mail.ru, ORCID: 0000-0002-2632-4439.
17 Grigorii O. Krylov, Dr. Sc. (Phys.-Math.), Professor, Prince Alexander Nevsky Military University of the Ministry of Defense of the Russian Federation, National Research Nuclear University MEPhI, Financial University under the Government of the Russian Federation, Moscow, Russia. E-mail: op50@mail.ru, ORCID: 0000-0001-8145-1994.

10. Shehab D. A., Alhaddad M. J. Comprehensive survey of multimedia steganalysis: Techniques, evaluations, and trends in future research // Symmetry. 2022; 14 (1). p. 117. https://doi.org/10.3390/sym14010117.
11. Stefan Kiltz, Jana Dittmann, Fabian Loewe, Christian Heidecke, Max John, Jonas Mädel and Fabian Preißler. 2024. Forensic Image Trace Map for Image-Stego-Malware Analysis: Validation of the Effectiveness with Structured Image Sets. In Proceedings of 2024 ACM 12th ACM Workshop on Information Hiding and Multimedia Security (ACM IH&MMSEC'24), June 24–26, 2024, Baiona, Spain. ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3658664.3659659.
12. Strachanski F., Petrov D., Schmidbauer T., Wendzel S. A Comprehensive Pattern-based Overview of Stegomalware // Proceedings of the 19th International Conference on Availability, Reliability and Security. 2024. pp. 1–10. https://doi.org/10.1145/3664476.3670886.
13. Volkhonskiy D., Nazarov I., Burnaev E. Steganographic generative adversarial networks // Twelfth international conference on machine vision (ICMV 2019). SPIE, 2020. V. 11433. pp. 991–1005. https://doi.org/10.48550/arXiv.1703.05502.