Научный вестник Орловского юридического института МВД России имени В.В. Лукьянова
№ 3(104) 2025 г.
Научная статья
УДК. 343.9

СОВРЕМЕННЫЕ СПОСОБЫ НЕПРАВОМЕРНОГО ВОЗДЕЙСТВИЯ НА КРИТИЧЕСКУЮ ИНФОРМАЦИОННУЮ ИНФРАСТРУКТУРУ РОССИЙСКОЙ ФЕДЕРАЦИИ

Колмыков Илья Александрович
Орловский юридический институт МВД России имени В. В. Лукьянова, Орёл, Россия

Ilyakolmykov01@mail.ru

Аннотация. Современное общество невозможно представить без информационных процессов, прочно вошедших во все сферы жизнедеятельности. Процессы общения, взаимодействия, трудовой деятельности на данном этапе развития общества трансформировались в вид компьютерной информации. Данная новелла является положительной стороной модернизации процессов облегчения взаимодействия и развития общества, однако следует констатировать, что с развитием технологий увеличиваются факты негативного и противоправного внешнего вмешательства в эти сферы жизнедеятельности со стороны преступных субъектов. Преступность трансформируется под социальные преобразования общества с целью расширения сфер своей противоправной деятельности, создаётся специальное программное обеспечение и видоизменяются существующие методы неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации.

Ключевые слова: криптография, стеганография, критическая информационная инфраструктура, способы, безопасность, информационные технологии, компьютерная информация.

Благодарности: работа выполнена при поддержке научного руководителя – профессора кафедры криминалистики и предварительного расследования в ОВД Орловского юридического института МВД России имени В. В. Лукьянова доктора юридических наук, доцента Калюжного А. Н.

Для цитирования: Колмыков И. А. Современные способы неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации // Научный вестник Орловского юридического института МВД России имени В. В. Лукьянова. 2025. № 3(104). С. 243–250.

MODERN WAYS OF UNLAWFUL INFLUENCE ON THE CRITICAL INFORMATION INFRASTRUCTURE OF THE RUSSIAN FEDERATION

Ilya A. Kolmykov
Lukyanov Orel Law Institute of the Ministry of the Interior of Russia, Orel, Russia

Ilyakolmykov01@mail.ru

Annotation. Modern society cannot be imagined without information processes that have become an integral part of their life. The processes of communication, interaction, and labor activity at this stage of society's development have transformed into a type of computer information. This novelty is a positive side of the modernization of the processes of facilitating interaction and development of society, however, it should be noted that with the

development of technology, the facts of negative and illegal external interference in these spheres of life by criminal entities are increasing. Crime is being transformed to meet changes in society in order to expand the scope of its illegal activities, special software is being created and existing methods of unlawful influence on the critical information infrastructure of the Russian Federation are being modified.

Keywords: cryptography, steganography, critical information infrastructure, methods, security, information technology, computer information.

Cratitude: the work was carried out with the support of the scientific supervisor – professor of the Department of Forensic Science and Preliminary Investigation in the Internal Affairs Directorate of the Oryol Law Institute of the Ministry of Internal Affairs of Russia named after V.V. Lukyanov, Doctor of Law, Associate Professor Kalyuzhny A.N.

For citation: Kolmykov I. A. Modern methods of unlawful influence on the critical information infrastructure of the Russian Federation // Scientific Bulletin of the Oryol Law Institute of the Ministry of Internal Affairs of Russia named after V.V. Lukyanov. 2025. № 3(104). P. 243–250.

Обращаясь к современным способам неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации, мы должны отметить, что противоправные субъекты активно прорабатывают сложно структурированные модели кибератак с использованием систем искусственного интеллекта, в связи с чем большинство исследователей и специалистов главным образом на теоретическом и практическом уровнях прорабатывают превентивные меры защиты, при этом на должном уровне не анализируют существующие способы [1, с. 429, 2, с. 279, 3, с. 17]. Так А. Н. Метелько справедливо отмечает, что с каждым годом многошаговые скоординированные распределённые кибератаки со сложной организацией, реализацией и множеством целей изменяются, проводятся всё чаще и изощрённее [4, с. 53].

Новым изощрённым способом является использование стеганографических и криптографических методов сокрытия элементов вирусного программного обеспечения в изображениях, аудио- или видеофайлах. Данные способы главным образом связаны с особенностью работы отечественного антивирусного программного обеспечения. Она заключается в том, что исследуется код картинки, аудио- или видеофайла, при этом не выявляется нарушение последовательности битов и их дополнительное встраивание, что открывает новые возможности для лиц, организаций и стран, осуществляющих неправомерные кибератаки на системы критической информационной инфраструктуры Российской Федерации.

Примерами такой деятельности являются события, связанные с неправомерным воздействием на промышленные компании Европы и Японии в 2020 году при помощи графических файлов с использованием *Mimikatz*. Для загрузки заражённых изображений атакующие субъекты использовали специальный скрипт на *PowerShell*. Алгоритм атаки заключался в следующем: специальный *PowerShell*-скрипт, используемый атакующими, загружает изображение с хостинга *Imgur* или *imgbox*. Этот медиафайл содержит данные, извлекая которые, вредоносная программа создаёт ещё один скрипт *PowerShell* – обфусцированную версию *Mimikatz*, после чего происходит несанкционированное копирование учётной записи и возможность полного доступа к ней. Считаем, что данный метод мог быть применён в том числе и на территории Российской Федерации.

Обозначив специфику и важность исследования способов неправомерного воздействия на критическую информационную инфраструктуру, перейдём к их анализу.

Первым анализируемым способом неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации будет стеганография. Начала современной стеганографии, как принято считать, заложил *GJ. Simmons* [5, с. 49].

Стеганография возникла в зарубежной практике благодаря анализу переписки двух заключённых, которые обменивались через открытые источники зашифрованной информацией под присмотром контролирующих лиц.

Современная информационная стеганография представляет собой вид компьютерной модернизации скрытого сообщения или размещение скрытого вируса на определённом формате (изображение, аудио- или видеофайл), который именуется «носитель информации». В настоящее время приобретает популярность такой формат носителя информации, как растровые и векторные изображения, аудио- и видеофайлы в меньшей степени адаптированы под задачи несанкционированного доступа к защищённой информации в связи со сложностью добавления (кодирования) дополнительных битов информации из-за существенного увеличения размера файла по сравнению с оригинальным. Стоит отметить, что раннее в качестве носителя информации использовались жёсткие диски и отдельные его пространственные файлы, однако с учётом усложнения инженерных способов защиты объектов критической информационной инфраструктуры и засекреченности данных о её информационных системах эта разновидность не используется.

Зарубежные исследователи считают, что субъект при передаче конфиденциальной информации, вирусов, содержащихся в изображениях, аудио- и видеофайлах, вставляет нужный ему элемент в наименее значимые её фрагменты файла, чтобы обычный обыватель не смог заметить скрытый смысл передаваемого сообщения и оно могло дойти до адресата, будучи нерасшифрованным [6; 7].

При этом рубежом защиты для зашифрованной передачи информации является сложность её распаковки и выявление конкретной передаваемой информации или вируса. Самый простой и быстрый способ уничтожить передаваемую (конфиденциальную) информацию – произвести её преобразование в иной формат или вернуть к исходному коду таким образом, чтобы зашифрованный участок изображения не имел ничего общего с изначальной передаваемой версией. Если даже один бит в информации передаваемого векторного изображения изменится, то смысловая передача зашифрованной информации исчезнет, то есть информация будет считаться уничтоженной. Так, если передаваемая информация была зашифрована в формат *JPEG* и затем преобразована в формат *TIFF*, а затем обратно в формат *JPEG*, даже если изображение выглядит точно так же для человеческого глаза, фактический состав битовой информации изображения отличается. В процессе возможного изменения файла лицом, которому стало известно о факте передачи информации или вируса при помощи стеганографии, но не обладающим информацией его конкретного расположения в передаваемом файле важно уяснить, какой именно способ стеганографии был применён.

Отметим противоправный пример использования и применения данной технологии. В 2019 году зарубежными и отечественными специалистами были выявлены уязвимости программы *Able2Extract Professional*, позволяющие выполнять код в системе через графические файлы в формате JPEG или BPM. Если пользователь откроет полученные картинки в ПО *Able2Extract Professional*, то скрытые в них команды будут записаны за пределами выделенной приложению области памяти (ОЗУ) и смогут выполнить любую команду внутри атакуемой системы. Данная зависимость возникла из-за протоколов проверки информации (детектирования) получаемой в виде расшифровки двоичных кодов всех получаемых файлов, кроме изображений в формате *JPEG*.

Вирус, содержащийся в передаваемом графическом файле, обладает большой глубиной передачи информации. Каждый пиксель – это набор параметров и, следовательно, набор битов. Человеческое восприятие не такое глубокое и чёткое, поэтому некритичное изменение бита не будет замечено при воспроизведении. Следовательно, часть бита может быть использована для доставки кода или текста. Полезная нагрузка может быть раскрыта загрузчиком, обрабатывающим полученный медиаконтент (как в примере с *Able2Extract Professional*), или использована для уязвимости в ПО.

Необходимо установить, что современные технологии сокрытия информации связаны с процессом стеганографии, поэтому проанализируем основные методы, применяемые в процессе сокрытия информации, а также выделим ключевые особенности их классификации и отграничения от иных технологий сокрытия информации.

Иными способы защиты передаваемой информации являются криптография и стеганография. Необходимо выделить ключевые особенности каждой технологии и отметить их качественные отличия.

Криптография представляет собой технологию защиты информации посредством шифрования данных с помощью математических и логических методов, поддающихся расшифровыванию с помощью открытого или закрытого ключа. Ключ – это набор данных, позволяющих правильно уяснить смысл передаваемой информации.

Как отмечают П. А. Волынкин и И. И. Смоляков, преимущество стеганографии над чистой криптографией состоит в том, что сообщения не привлекают к себе внимания. Сообщения, факт шифрования которых не скрыт, вызывают подозрение и могут быть сами по себе уличающими в тех странах, в которых запрещена криптография [8, с. 61]. Таким образом, криптография защищает содержание сообщения, а стеганография защищает сам факт наличия каких-либо скрытых посланий. Стенография представляет собой совокупность методов быстрой записи информации посредством системы знаков. Сочетание применения специальных систем знаков и сокращений передаваемой информации является процессом закрытого шифрования, то есть передачи сведений для конкретного лица, обладающего знаниями в этой области. Стеганография отличается от данного метода тем, что она не подразумевает шифрование информации.

Рассмотрим подробным образом существующие методы стеганографии для сокрытия информации в изображениях, а именно: метод наименее значимого бита (*LSB*), *PVD*-стеганография, дискретное косинусное преобразование (*DCT*), дискретно вейвлет-преобразование (*DWT*).

Метод наименее значимого бита считается самым простым и в то же время уникальным способом скрытой передачи информации. Принцип работы основан на использовании одних битов информации на другие. Из школьного курса предмета информатики мы знаем, что классическая адаптивная цветовая модель (*RGB*) состоит из битов, которые создают пиксели, используемые для сочетания цветов и образующие цветовую палитру, предназначенную для создания изображения. Основываясь на анализе биологических и физиологических возможностей человеческого зрения, мы приходим к выводу о том, что человеческий глаз, воспринимающий внешний облик предмета или окружающую среду, передаёт эту информацию в мозг, который формирует уже целую картинку. Однако существуют ограничения восприятия цветовой палитры человеком (человеческий глаз способен воспринимать лишь небольшой диапазон электромагнитного спектра – от 380 до 760 нанометров), за счёт увеличения или уменьшения спектра возможно передавать информацию открытым способом так, чтобы человек не смог её уловить. Для этих целей можно использовать растровое и векторное изображения.

Принцип работы данного метода основан на замене одного цвета на наиболее приближенный к нему.

Данная технология применяется для защиты авторского права на изображение либо передачи информации для группы лиц анонимным пользователем. Отмечаем преимущество и недостатки данного метода. Преимуществом является быстрый способ создания изображения с передаваемой информации большого объёма посредством использования таких программ, как *Steghide, OpenStego, SSuite Picsel, SilentEye SteganoGAN* и другие. Недостатком метода является низкий уровень защищённости, возможность удаления передаваемой информации при форматировании формата изображения. Вторым недостатком является узкий формат применяемых изображений: *BMP, PNG* (без сжатия), *GIF* (сжатием).

PVD-метод стеганографии является более сложным и защищённым способом сокрытия. Он основан на принципе вычисления разницы между определённой областью (значением) соседних пикселей с последующей их модификацией с целью встраивания битов скрытой информации. Для его работы необходимо использование младших битов в пикселях, у которых яркость сильнее отличается от соседних. Алгоритм передачи скрытой информации задействует визуальную разность искажения изображения и увеличения вместимости изображений-контейнера.

Недостатком метода считается сложность реализации передачи скрываемой информации с возможностью его обнаружения современными методиками стеганоанализа.

Дискретное косинусное преобразование является третьим методом стеганографии. Дискретное косинусное преобразование оперирует блоками изображения или блоками вычетов X размера N × N и подаёт на выход блоки коэффициентов Y такого же размера. Данный метод устойчив к сжатию изображения и не зависит от качества исходного изображения. Его преимуществом является возможность применения ко всем областям изображения, а не только к отдельным областям.

Дискретное вейвлет-преобразование (*DWT*) – это ещё одна частотная область, в которой может быть реализована стеганография. *DCT* рассчитывается на блоках независимых пикселей, ошибка кодирования вызывает разрыв между блоками, что приводит к раздражающему артефакту блокировки. Этот недостаток *DCT* устраняется с помощью DWT. DWT применяется ко всему изображению. *DWT* обеспечивает лучшее уплотнение энергии, чем DCT, без каких-либо артефактов блокировки. *DWT* разделяет компонент на многочисленные частотные полосы, называемые подполосами, известными как:

a) LL – горизонтально и вертикально низкие частоты,

b) LH – горизонтально низкие частоты и вертикально высокие частоты,

c) HL – горизонтально высокие частоты и вертикально низкие частоты,

d) HH – горизонтально и вертикально высокие частоты,

e) поскольку человеческие глаза гораздо более чувствительны к низкочастотной части (подполоса LL), мы можем скрыть секретное сообщение в трёх других частях, не внося никаких изменений в подполосу LL. Поскольку другие три подполосы являются высокими частотами, они содержат незначительные данные. Скрытие секретных данных в этих поддиапазонах не так уж сильно ухудшает качество изображения. *DWT,* используемый в этой работе, – это *Haar-DWT*, простейший *DWT* [9].

Рассмотрев основные методы стеганографии, необходимо уяснить алгоритм передачи информации в векторных изображениях.

1. Изменение атрибутов элементов представляет собой способ кодирования данных через небольшие модификации характеристик графических элементов. Например, корректировка координат точек или толщины линий может использоваться для передачи информации. Важно соблюдать баланс изменений, чтобы не нарушить визуальное восприятие изображения.

2. Добавление невидимых объектов позволяет использовать прозрачные фигуры или линии для хранения данных. Присутствие или отсутствие определённых элементов может кодировать биты информации (0 или 1), которые будут оставаться при этом незаметным для наблюдателя.

3. Работа с атрибутами цвета даёт возможность кодировать информацию через незначительные изменения параметров цвета и прозрачности векторных объектов, что отличается от методов растровой стеганографии.

4. Структурное кодирование использует текстовые свойства и комментарии XML в форматах типа SVG. Невидимые для пользователя элементы, такие как метки и комментарии, могут содержать скрытые сообщения.

5. Управление контейнерами и слоями позволяет встраивать информацию в дополнительные слои или группы, которые не отображаются при обычном просмотре изображения.

Такой подход обеспечивает надёжное встраивание информации при сохранении визуального качества исходного изображения. Случайный порядок встраивания и использование криптографического хэширования повышают устойчивость метода к несанкционированному извлечению данных.

С целью выявления зашифрованный информации и вирусов возможно применение следующих методов стеганоанализа, представленных на рисунке 1 [10, с. 130].

Рис.1. Основные методы выявления стеганографии

Таким образом, в рамках анализа современных способов неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации нами были затронуты в основном стеганографические и криптографические методы встраивания сокрытой информации и вирусов в изображениях, картинках. Освещение упомянутых ранее способов главным образом связано с выявлением со стороны лиц, организаций, стран, осуществляющих противоправную деятельность против интересов и национальной безопасности Российской Федерации, уязвимостей работы антивирусного программного обеспечения. Кроме этого, конечной целью использования стеганографических и криптографических методов мы видим дестабилизацию работы критической информационной инфраструктуры и выявление новых уязвимостей, необходимых для несанкционированной обработки и пересылки массива данных о её работе. С учётом обозначенного считаем, что необходимо детальным образом проработать новые методики стеганоанализа.

1. Прокопьева Т. В., Больнова Н. С., Давлетова А. И., Липявко Е. С. Влияние искусственного интеллекта на экономическую безопасность в условиях цифровизации // Экономическая безопасность страны, регионов, организаций различных видов деятельности : Материалы V Всероссийского форума в Тюмени по экономической безопасности, Тюмень, 24–27 апреля 2024 года. Тюмень: ТюмГУ-Press, 2024. С. 425–431.
2. Метельков А. Н. Киберучения: зарубежный опыт защиты критической инфраструктуры // Правовая информатика. 2022. № 1. С. 51–60.

3. Стародубцева Е. А. Влияние искусственного интеллекта на информационную безопасность // Цифровая экономика и финансы: Материалы VIII Международной научно-практической конференции, Санкт-Петербург, 20–21 марта 2025 года. СПб: Центр научно-информационных технологий "Астерион", 2025. С. 278–281.
4. Лощилин А. В. Роль и значение искусственного интеллекта в обеспечении безопасности информационных систем: перспективы и вызовы // НБИ технологии. 2024. Т. 18, № 4. С. 16–20.
5. Голубев Е. А. Стеганографические технологии - новое направление защиты информации // T-Comm: Телекоммуникации и транспорт. 2012. Т. 6, № 6. С. 49–53.
6. Balaji, R., & Naveen, G. (2011). Secure data transmission using video Steganography. In 2011 IEEE International Conference on Electro/Information Technology, IEEE, pp. 1–5.
7. Vijayakumar, P., Azees, M., Kannan, A., & Deborah, L. J. (2015). Dual authentication and key management techniques for secure data transmission in vehicular ad hoc networks. IEEE Transactions on Intelligent Transportation Systems, 17(4), 1015–1028.
8. Волынкин П. А. Эффективность хранения контента в графических контейнерах при стеганографии // Современная наука: актуальные вопросы, достижения и инновации : сборник статей VII Международной научно-практической конференции : в 4 ч., Пенза, 05 июня 2019 года. Том Часть 2. Пенза: "Наука и Просвещение" (ИП Гуляев Г.Ю.), 2019. С. 60–64.
9. DWT Technique for Steganography // Academia. edu URL: https://www.academia.edu/12745731/DWT_Technique_for_Steganography (дата обращения: 17.03.2025).
10. Николаенко В. Г. Алгоритм стеганоанализа для оценки качества алгоритма встраивания информации // Евразийский союз ученых. 2015. № 5-3(14). С. 129–130.

1. Prokop`eva T. V., Bol`nova N. S., Davletova A. I., Lipyavko E. S. Vliyanie iskusstvennogo intellekta na e`konomicheskuyu bezopasnost` v usloviyax cifrovizacii // E`konomicheskaya bezopasnost` strany`, regionov, organizacij razlichny`x vidov deyatel`nosti : Materialy` V Vserossijskogo foruma v Tyumeni po e`konomicheskoj bezopasnosti, Tyumen`, 24–27 aprelya 2024 goda. Tyumen`: TyumGU-Press, 2024. S. 425–431.
2. Metel`kov A. N. Kiberucheniya: zarubezhny`j opy`t zashhity` kriticheskoj infrastruktury` // Pravovaya informatika. 2022. № 1. S. 51–60.
3. Starodubceva E. A. Vliyanie iskusstvennogo intellekta na informacionnuyu bezopasnost` // Cifrovaya e`konomika i finansy`: Materialy` VIII Mezhdunarodnoj nauchno-prakticheskoj konferencii, Sankt-Peterburg, 20–21 marta 2025 goda. SPb: Centr nauchno-informacionny`x texnologij Asterion, 2025. S. 278–281.
4. Loshhilin A. V. Rol` i znachenie iskusstvennogo intellekta v obespechenii bezopasnosti informacionny`x sistem: perspektivy` i vy`zovy` // NBI texnologii. 2024. T. 18, № 4. S. 16–20.
5. Golubev E. A. Steganograficheskie texnologii - novoe napravlenie zashhity` informacii // T-Comm: Telekommunikacii i transport. 2012. T. 6, № 6. S. 49–53.
6. Balaji, R., & Naveen, G. (2011). Secure data transmission using video Steganography. In 2011 IEEE International Conference on Electro/Information Technology, IEEE, pp. 1–5.
7. Vijayakumar, P., Azees, M., Kannan, A., & Deborah, L. J. (2015). Dual authentication and key management techniques for secure data transmission in vehicular ad hoc networks. IEEE Transactions on Intelligent Transportation Systems, 17(4), 1015–1028.
8. Voly`nkin P. A. E`ffektivnost` xraneniya kontenta v graficheskix kontejnerax pri steganografii // Covremennaya nauka: aktual`ny`e voprosy`, dostizheniya i innovacii : sbornik

statej VII Mezhdunarodnoj nauchno-prakticheskoj konferencii : v 4 ch., Penza, 05 iyunya 2019 goda. Tom Chast` 2. Penza: Nauka i Prosveshhenie (IP Gulyaev G.Yu.), 2019. S. 60–64.
9. DWT Technique for Steganography // Academia.edu URL: https://www.academia.edu/12745731/DWT_Technique_for_Steganography (data obrashheniya: 17.03.2025).
10. Nikolaenko V. G. Algoritm steganoanaliza dlya ocenki kachestva algoritma vstraivaniya informacii // Evrazijskij soyuz ucheny`x. 2015. № 5-3(14). S. 129–130.

Информация об авторе

Илья Александрович Колмыков. Адъюнкт.
Орловский юридический институт МВД России имени В. В. Лукьянова.
302027, Россия, г. Орёл, ул. Игнатова, 2.

Information about the author

Ilya A. Kolmykov. Adjunct.
Lukyanov Orel Law Institute of the Ministry of the Interior of Russia.
302027, Russia, Orel, Ignatov Str., 2.

Статья поступила в редакцию 23.06.2025; одобрена после рецензирования 15.09.2025; принята к публикации 29.09.2025.
The article was received in the editorial office on 23.06.2025; approved after review on 15.09.2025; accepted for publication on 29.09.2025.