Научная статья
УДК 343.985.7:343.34:004

Андрей Дмитриевич Абаринов
Нижегородская академия МВД России, Нижний Новгород, Россия, abarinovandrew@gmail.com

КРИМИНАЛИСТИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ВЫЯВЛЕНИЯ И РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ ЭКСТРЕМИСТСКОЙ И ТЕРРОРИСТИЧЕСКОЙ НАПРАВЛЕННОСТИ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ СТЕГАНОГРАФИИ

Аннотация. В статье рассмотрены вопросы использования объектов, преобразованных с помощью стеганографии, при осуществлении преступной деятельности экстремистской и террористической направленности. Дана краткая характеристика стеганографического способа сокрытия информации, в том числе в иллюстративной форме. Отмечено, что использование стеганографического способа сокрытия информации в силу своей специфики может усложнить процесс выявления, раскрытия и расследования преступлений. Из практики зарубежных правоохранительных органов приведены примеры использования стеганографии в преступной деятельности. Отражены цифровые свойства и следы, которые могут иметь криминалистически значимую и доказательственную информацию. В заключение автор приходит к выводу о необходимости акцентирования внимания на важности разработки новых и совершенствовании уже существующих методов стеганоанализа, а также формирования концептуальных основ обнаружения, фиксации и изъятия цифровых следов.

Ключевые слова: преступления экстремистской и террористической направленности, выявление, расследование, следовая картина, стеганография, стеганоанализ, цифровая криминалистика

Для цитирования: Абаринов А. Д. Криминалистическое обеспечение выявления и расследования преступлений экстремистской и террористической направленности, совершаемых с использованием стеганографии // Общество, право, государственность: ретроспектива и перспектива. 2025. № 3 (23). С. 28–35.

Original article

Andrey D. Abarinov
Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia, Nizhny Novgorod, Russia, abarinovandrew@gmail.com

FORENSIC SUPPORT FOR THE DETECTION AND INVESTIGATION OF EXTREMIST AND TERRORIST CRIMES COMMITTED USING STEGANOGRAPHY

Abstract. The article considers the issues of using objects transformed by steganography in committing extremist and terrorist crimes. It gives a brief description of the steganographic method of concealing information, including in illustrative form. It is noted that the use of the steganographic method of concealing information, due to its specificity, can complicate the process of identifying, solving and investigating crimes. Examples of using steganography in criminal activities are given from the practice of foreign law enforcement agencies. Digital properties and traces that can have forensically significant and evidentiary information are reflected. Finally, the author comes to the conclusion about the need to focus on the importance of developing

new and improving existing steganalysis methods, as well as the formation of conceptual foundations for detecting, recording and seizing digital traces.

Key words: extremist and terrorist crimes, detection, investigation, trace picture, steganography, steganalysis, digital forensics

For citation: Abarinov A. D. Forensic support for the detection and investigation of extremist and terrorist crimes committed using steganography // Society, law, statehood: retrospective and perspective. 2025. No. 3 (23). P. 28–35. (In Russ.)

Введение

В эпоху цифровизации информация стала главной валютой, а ее защита – критически важной задачей. Стеганография, древнее искусство скрытия сообщений, сегодня переродилась в мощный инструмент кибербезопасности и одновременно в средство осуществления преступной деятельности. В современных условиях совершение преступлений экстремистского и террористического характера сопровождается активным использованием информационно-телекоммуникационных технологий. Преступные организации и сообщества активно внедряют новые методы скрытой коммуникации, одним из которых является стеганография. Указанная криминальная активность характеризуется наличием цифровых следов, исследование которых, как было отмечено нами ранее [1], требует у субъекта деятельности по выявлению и расследованию преступлений наличия специальных знаний. Данные следы могут содержать криминалистически релевантную информацию, обнаружение которой будет способствовать более эффективному выявлению, раскрытию и расследованию преступлений.

Методы

В исследовании использовались общенаучные методы, основанные на диалектическом подходе. Для обеспечения системности применены эмпирико-теоретические, формально-логические методы обобщения, систематизации и классификации. Исторический метод использован для изучения эволюции стеганографии. Описание некоторых процессов и явлений, связанных с возникновением цифровых свойств и следов, проведено с использованием анализа и синтеза признаков отдельных понятий и явлений.

Результаты

Стеганография (от греч. «скрытое письмо») представляет собой способ передачи или сохранения информации, ориентированный на сокрытие самого факта существования передаваемой или хранимой информации. Самая ранняя известная техника стеганографии была разработана в Древней Греции около 440 г. до н. э. В трактате древнегреческого историка Геродота Histories («История») содержится описание одного из первых примеров стеганографии – эпизода, связанного с Гистиеем Милетским, который использовал такой метод для передачи секретного послания во время Ионийского восстания против Персии. Так, согласно изложенным в трактате данным, голову раба побрили, а затем на коже головы нанесли татуировку. Когда волосы раба отросли и скрыли татуировку, его отправили к получателю. Получатель снова побрил голову раба и получил послание [2].

В отличие от криптографии, которая защищает содержание сообщения, стеганография маскирует сам факт его существования. Тем не менее, как справедливо подчеркивал П. А. Фаниев, стеганография используется в сочетании с криптографическими методами, усиливая их и таким образом увеличивая степень безопасности передаваемой информации [3, с. 76]. Данный способ оперирует различными носителями информации: изображениями (JPEG, PNG и др.); аудиофайлами (MP3 и др.); видео (MP4 и др.); текстовыми документами (TXT, DOCX и др.); сетевыми протоколами (TCP, UDP, ICMP и др.) [4]. Также, как было отмечено рядом авторов, в настоящее время в качестве носителя секретной информации может быть использован файл любого типа (даже заголовок IP-пакета), то есть скрытая (дополни-

тельная) информация может быть встроена в любой файл, если он занимает больше места, чем требуется для его хранения[1].

К основным методам стеганографии можно отнести следующие:

1) LSB (Least Significant Bit) – замена наименее значимых битов в пикселях изображения;

2) спектральное скрытие – внедрение данных в частотные характеристики аудиосигналов;

3) структурные модификации – изменение метаданных файлов.

Как было отмечено индийским ученым К. Чоудхари, во всех стеганографических методах используются маскирующий объект и стеганографический объект. Маскирующий объект – это объект, используемый в качестве носителя для встраивания в него сообщений. В современном контексте в качестве маскирующих объектов применяются изображения, файловые системы и проч. В качестве объектов-замаскировок могут использоваться системы, аудиофайлы, видеофайлы, а также HTML-страницы и даже спам-письма. Стеганографический объект – это объект, несущий скрытое сообщение [5, с. 34].

Не ставя в рамках настоящего исследования цели глубокого анализа программно-технических аспектов способов стеганографии, для лучшего понимания наглядно представим способ сокрытия фрагмента текстового материала с использованием стеганографии (рис.).

Использование стеганографического способа сокрытия информации в силу своей специфики может усложнить процесс выявления, раскрытия и расследования отдельных видов преступлений, в том числе экстремистской и террористической направленности. Справедливо, на наш взгляд, согласиться с суждением о том, что в ряде случаев использование данного способа сокрытия следов преступления может оказаться для следователя неожиданным и в итоге он может не обратить внимания на важную для расследования информацию [6, с. 200].

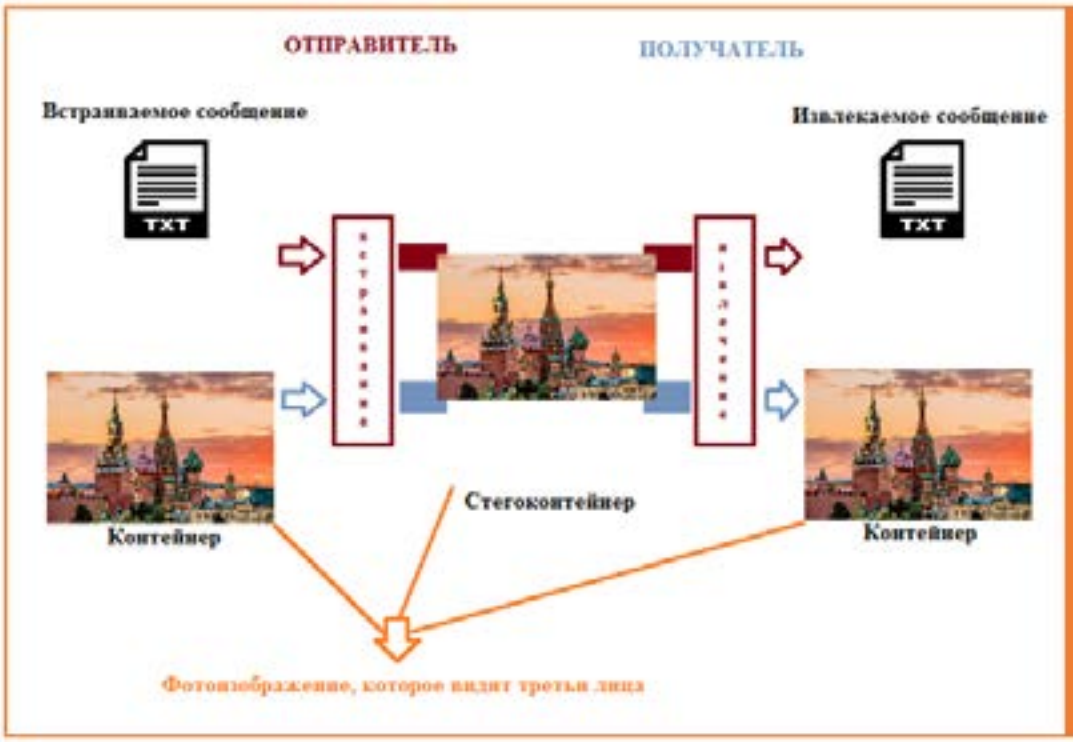

Рис. Стеганографический способ сокрытия текста

[1] Крыгин С. В., Сухов С. Н., Чикина Т. Е.Основы информационной безопасности и защита информации в ОВД : учеб.-практ. пособие / МВД России, НА. Н. Новгород : НА МВД России, 2018. С. 57.

По мнению американского криптографа, специалиста по компьютерной безопасности Б. Шнайера, стеганография – это хороший способ связи для террористических ячеек, позволяющий осуществлять общение без раскрытия личности представителей другой группы. Еще в 2001 г. им отмечено, что по имеющейся информации, полученной от компетентных должностных лиц зарубежных правоохранительных органов, террористические группы скрывают карты и фотографии своих преступных целей и размещают инструкции по террористической деятельности в спортивных чатах, на порнографических сайтах объявлений и других веб-сайтах[1].

В своей работе сербский ученый Д. Трифунович также отмечает, что террористы обычно шифруют сообщения, применяя программы шифрования с открытым исходным кодом, которые включают методы стеганографии, и размещают скрытые сообщения на фотографиях, видео или в тексте практически на любом веб-сайте или напрямую отправляют по электронной почте [7]. Исследователь подкрепляет свои доводы примерами из судебно-следственной практики европейских правоохранительных органов, ссылаясь на материалы, опубликованные CNN[2] и Die Zeit[3].

Так, один из случаев использования стеганографии исламскими террористами выявлен, когда в мае 2011 г. в Берлине был задержан предполагаемый член «Аль-Каиды»[4] Максуд Лодин, 22-летний австриец.

М. Лодин направлялся в Берлин из Пакистана через Венгрию, когда его задержали сотрудники берлинской полиции. В его нижнем белье обнаружили USB-накопитель, содержащий видео порнографического характера. Эксперты по компьютерной криминалистике из Федеральной уголовной полиции Германии извлекли из данного видео 141 скрытый текстовый файл, в котором подробно описывались операции «Аль-Каиды» и планируемые террористические акции. В изъятых файлах содержались планы атак круизных судов, используемых как отвлекающий маневр в то время, пока в Европе проводились бы другие террористические акты. Также были обнаружены руководства по подготовке террористов в формате PDF на немецком, английском и арабском языках. Файлы были спрятаны внутри видео с использованием техники цифровой стеганографии, но не зашифрованы [7].

Указанный пример приводит к выводу о том, что последователи транснациональных террористических и экстремистских формирований уже давно при осуществлении преступной деятельности используют возможности научно-технологического прогресса, в том числе стеганографические способы скрытой коммуникации.

Принимая во внимание тот факт, что процесс идентификации скрытой информации включает решение трех взаимосвязанных задач: локализации скрытой информации (обнаружение закладки), классификации ее формата, последующей идентификации данных, можно утверждать о том, что каждый этап представляет собой критически важную составляющую для успешного извлечения и анализа искомых сведений.

При наличии соответствующих технических средств анализа и обработки данных возможно выявление остаточных цифровых следов, указывающих на присутствие скрытых объектов (закладок). Эта стадия, которую можно именовать как «детекция при-

[1] Terrorists and steganography = Террористы и стеганография // ZDNET. URL: https://www.zdnet.com/article/terrorists-and-steganography/ (дата обращения: 06.12.2024).

[2] Documents reveal al Qaeda's plans for seizing cruise ships, carnage in Europe = Документы раскрывают планы «Аль-Каиды» по захвату круизных судов и резне в Европе // EDITION.CNN. URL: https://edition.cnn.com/2012/04/30/world/al-qaeda-documents-future/ (дата обращения: 06.12.2024).

[3] Steganography: how al-Qaeda hid secret documents in a porn video = Стеганография: как «Аль-Каида» спрятала секретные документы в порновидео // Arstechnica. URL: https://arstechnica.com/information-technology/2012/05/steganography-how-al-qaeda-hid-secret-documents-in-a-porn-video/ (дата обращения: 06.12.2024).

[4] Организация, деятельность которой запрещена на территории Российской Федерации.

сутствия», представляет собой начальный этап контрмер по борьбе со стеганографией.

При исследовании следовой картины объектов, преобразованных с использованием стеганографии, важно понимать, что стеганография направлена на сокрытие информации внутри других объектов (фото-, видео-, текстовых и иных материалов) таким образом, чтобы ее наличие было трудно обнаружить. Именно в этом и проявляется нетривиальность механизма следообразования. При этом согласимся с позицией М. М. Льянова: необходимо учитывать возможность выборочной стеганографии, что следует проверять путем выявления закономерностей в использовании данного способа сокрытия преступления в каждом конкретном случае [8, с. 120].

Н. С. Зиновьевой отмечено, что «...скрытая обозначенными методами информация формирует специфическую следовую картину в математической форме с определенным набором знаков» [9, с. 89].

В рамках настоящего исследования нами установлено, что криминалистическую и доказательственно важную информацию могут иметь следующие цифровые следы и свойства:

1. Метаданные объекта, преобразованного методом стеганографии (цифровой след), – структурированная информация, описывающая свойства файла-контейнера (например, дата создания, формат, параметры обработки), которая может сохранять следы модификации, связанные с внедрением скрытых данных. Включают как исходные метаданные, частично сохранившиеся после стеганографического преобразования, так и новые данные, сгенерированные инструментами стеганографии (например, отметки о программном обеспечении, изменение размера файла или хеш-суммы).

2. Статистические аномалии в объекте, преобразованном методом стеганографии (цифровое свойство), – отклонения в распределении ключевых характеристик носителя (пикселей, аудиосэмплов, битовых последовательностей) от естественных статистических закономерностей, свойственных исходному типу файла. Возникают из-за внедрения скрытых данных, нарушающих энтропию, корреляцию между соседними элементами или частоту встречаемости значений (например, искажение гистограммы изображения или аномальное распределение младших битов в аудиофайле).

3. Артефакты сжатия объекта, преобразованного методом стеганографии (цифровое свойство), – визуальные или структурные искажения, вызванные несовместимостью алгоритмов сжатия (например, JPEG, MP3) с модификациями при стеганографии. Проявляются как повторное сжатие файла с потерей качества, несоответствие таблиц квантования, блоковые артефакты в изображениях или аномалии в частотных компонентах, которые не характерны для исходного процесса компрессии.

4. Ошибки квантования объекта, преобразованного методом стеганографии (цифровое свойство), – несоответствия в значениях квантованных коэффициентов (например, в JPEG – коэффициенты дискретного косинусного преобразования), возникающие при внедрении скрытых данных в уже сжатый файл. Проявляются как отклонения от ожидаемых шаблонов квантования, неравномерное распределение остатков или аномалии в младших битах, которые могут быть выявлены методами анализа гистограмм или машинного обучения.

5. Аномалии частотного спектра сигналов объекта, преобразованного методом стеганографии (цифровое свойство), – искажения в частотной области носителя (изображение, аудио, видео), вызванные внедрением скрытой информации. Включают нехарактерные пики, сдвиги в энергетическом спектре, нарушения гармоничности сигнала или аномалии в высокочастотных компонентах, выявляемые с помощью преобразования Фурье, вейвлет-анализа или методов стеганодетекции, ориентированных на спектральные особенности.

Как ранее уже было отмечено в работе А. Л. Осипенко и А. И. Гайдина, текстовая информация может быть зашифрована или скрытно размещена в файлах иных типов с использованием методов стеганографии. Для ее выявления потребуется применение

Таблица

Инструменты для обнаружения стеганографии и анализа данных

Название инструмента	Назначение	Методы
StegExpose	Обнаружение стеганографии в изображениях (JPEG, PNG, BMP)	Анализ LSB, статистические тесты (χ^2)
Stegdetect	Выявление данных, скрытых с помощью инструментов (JSteg, JPHide, OutGuess)	Эвристический анализ коэффициентов DCT в JPEG
AperiSolve	Многослойный анализ изображений (включая стего, метаданные, EXIF)	Цветовые каналы, частотные домены
StegoHunter	Анализ изображений, аудио и видео	Сигнатурный и поведенческий анализ
Ghiro	Автоматизированный анализ изображений	Проверка целостности, поиск скрытых данных
Digital Invisible Ink Toolkit (DIIT)	Обнаружение и извлечение данных, скрытых с помощью LSB	Анализ цветовых каналов
OpenStego	Обнаружение и извлечение данных в изображениях	Проверка водяных знаков и LSB
Wireshark	Анализ сетевого трафика на предмет передачи стегофайлов	Фильтрация по MIME-типам, аномальным размерам пакетов
DeepSound	Обнаружение данных, скрытых в аудиофайлах (WAV, MP3)	Анализ спектрограмм
CNNs	Классификация файлов с использованием нейросетей	Обучение на датасетах с помеченными стегообъектами

алгоритмов криптоанализа и стеганоанализа в лабораторных условиях при проведении специализированных экспертиз [10, с. 160]. В связи с этим инструменты цифровой криминалистики в целом и передовые инструменты стеганоанализа в частности имеют решающее значение [11]. Для обнаружения объектов, преобразованных методом стеганографии, применяются методы стегоанализа, направленные на выявление скрытых данных. Современные программные решения сочетают традиционные алгоритмы (например, анализ наименее значащих битов – LSB) с инновационными подходами, такими как нейронные сети (табл.).

Заключение

В результате проведенного в рамках представленной статьи исследования сделаны следующие выводы.

Установлено, что использование стеганографии при совершении преступлений экстремистской и террористической направленности проявляется в нетривиальности механизма следообразования. Так, стеганография направлена на сокрытие информации внутри других объектов (фото-, видео-, текстовых и иных материалов) таким образом, чтобы ее наличие было трудно обнаружить.

Определены виды цифровых свойств (статистические аномалии, артефакты сжа-

тия, ошибки квантования, аномалии частотного спектра сигналов) и следов (метаданные) объектов, преобразованных методом стеганографии, которые могут содержать криминалистически значимую информацию.

Для дальнейшего эффективного выявления, раскрытия и расследования преступлений экстремистской и террористической направленности необходима разработка новых и совершенствование уже существующих методов стеганоанализа, в том числе применение стегоанализа при проведении судебно-компьютерных экспертиз, а также формирование концептуальных основ обнаружения, фиксации и изъятия цифровых следов.

СПИСОК ИСТОЧНИКОВ

1. Абаринов А. Д. Следовая картина преступлений экстремистской направленности // Аграрное и земельное право. 2024. № 6 (234). С. 298–300.

2. Herodotus. The Histories. Vol. 3, Books 5–7 (with an English translation by Godley A. D.). Cambridge : Harvard University Press, 1922. Vol. 3 (5). P. 50–51.

3. Фаниев П. А. О некоторых способах обнаружения стегосообщений с использованием языка программирования Python // Вестник Краснодарского университета МВД России. 2024. № 1 (63). С. 76–79.

4. Федосенко М. Ю., Беззатеев С. В. Анализ проблематики применения методов стеганографии при осуществлении противоправных действий и ее роли в цифровой криминалистике // Проблемы информационной безопасности. Компьютерные системы. 2023. № 3 (56). С. 33–57.

5. Choudhary K. Image steganography and global terrorism // International Journal of Scientific & Engineering Research. 2012. Vol. 3, issue 7. P. 34–48. https://doi.org/10.9790/0661-0123448.

6. Смахтин Е. В., Льянов М. М. Сокрытие электронно-цифровых следов как способ противодействия расследованию преступлений // Технологии XXI века в юриспруденции : материалы Пятой междунар. науч.-практ. конф. (Екатеринбург, 19 мая 2023 г.). Екатеринбург : АНО «Центр содействия развитию криминалистики “КримЛиб”», 2023. С. 195–203.

7. Trifunovic D. Digital steganography in terrorist networks // SYM-OP-IS 2015: XLII International Symposium on Operations Research. 2015. Vol. V (1).

8. Льянов М. М. Криминалистическое значение электронно-цифровых следов преступлений экстремистской и террористической направленности в сети «Интернет» : дис. ... канд. юрид. наук. Тюмень, 2024. 248 с.

9. Зиновьева Н. С. К вопросу о месте криптографии и стеганографии в криминалистической науке // Гуманитарные, социально-экономические и общественные науки. 2019. № 2. С. 87–89.

10. Осипенко А. Л., Гайдин А. И. Правовое регулирование и тактические особенности изъятия электронных носителей информации // Вестник Воронежского института МВД России. 2014. № 1. С. 156–163.

11. Nicolas-Sanchez A., Castro-Toledo F. J. Uncovering the social impact of digital steganalysis tools applied to cybercrime investigations: a European Union perspective // Crime Science. 2024. Vol. 13:11. https://doi.org/10.1186/s40163-024-00209-7.

REFERENCES

1. Abarinov A. D. The trace pattern of extremist crimes // Agrarian and land law. 2024. No. 6 (234). P. 298–300. (In Russ.)

2. Herodotus. The Histories. Vol. 3, Books 5–7 (with an English translation by Godley A. D.). Cambridge : Harvard University Press, 1922. Vol. 3 (5). P. 50–51.

3. Faniev P. A. About some ways detecting stego messages using the Python programming language // Bulletin of Krasnodar University of Russian MIA. 2024. No. 1 (63). P. 76–79. (In Russ.)

4. Fedosenko M. Yu.? Bezzateev S. V. Analysis of the problems of using steganography methods in the implementation of illegal actions and its role in digital forensics // Information security problems. Computer systems. 2023. No. 3 (56). P. 33–57. (In Russ.)

5. Choudhary K. Image steganography and global terrorism // International Journal of Scientific & Engineering Research. 2012. Vol. 3, issue 7. P. 34–48. https://doi.org/10.9790/0661-0123448.

6. Smakhtin E. V., Lyanov M. M. Concealment of electronic digital traces as a way to counteract the investigation of crimes // Technologies of the 21st century in jurisprudence : materials of the Fifth international scientific and practical conference (Ekaterinburg, May 19, 2023). Ekaterinburg : ANO "Center for Assistance to the Development of Criminalistics "KrimLib", 2023. P. 195–203. (In Russ.)

7. Trifunovic D. Digital steganography in terrorist networks // SYM-OP-IS 2015: XLII International Symposium on Operations Research. 2015. Vol. V (1).

8. Lyanov M. M. Forensic significance of electronic-digital traces of crimes of extremist and terrorist orientation on the Internet : dis. ... Cand. of Law. Tyumen, 2024. 248 p. (In Russ.)

9. Zinovieva N. S. About the place of cryptography and steganography in forensic science // Humanities, social-economic and social sciences. 2019. No. 2. P. 87–89. (In Russ.)

10. Osipenko A. L., Gaidin A. I. Legal regulation and tactical features of seizure of electronic data media // Bulletin of Voronezh Institute of the Ministry of the Interior of Russia. 2014. No. 1. P. 156–163. (In Russ.)

11. Nicolas-Sanchez A., Castro-Toledo F. J. Uncovering the social impact of digital steganalysis tools applied to cybercrime investigations: a European Union perspective // Crime Science. 2024. Vol. 13: 11. https://doi.org/10.1186/s40163-024-00209-7.

Информация об авторе:
Абаринов А. Д. – адъюнкт.

Information about the author:
Abarinov A. D. – adjunct.

Статья поступила в редакцию 11.04.2025; одобрена после рецензирования 03.06.2025; принята к публикации 26.09.2025.

The article was submitted 11.04.2025; approved after reviewing 03.06.2025; accepted for publication 26.09.2025.