https://doi.org/10.30764/1819-2785-2024-4-95-101

Новые публикации по судебной экспертизе

Н.В. Фетисенкова, Д.В. Василевская
Федеральное бюджетное учреждение Российский федеральный центр судебной экспертизы имени профессора А.Р. Шляхова при Министерстве юстиции Российской Федерации, Москва 101000, Россия

Аннотация. Представлены переводы рефератов избранных статей, опубликованных в периодических изданиях: Journal of Forensic Sciences [www.wileyonlinelibrary.com/journal/jfo], Forensic Science International [www.elsevier.com/locate/forsciint], Forensic Science International: Digital Investigation [www.elsevier.com/locate/j.fsidi], Forensic Science International: Reports [www.elsevier.com/locate/j.fsir], Science & Justice [www.elsevier.com/locate/j.scijus].

New Publications in Forensic Science

Natal'ya V. Fetisenkova, Dar'ya V. Vasilevskaya
The Russian Federal Centre of Forensic Science named after professor A.R. Shlyakhov of the Ministry of Justice of the Russian Federation, Moscow 101000, Russia

Abstract. This section presents translated abstracts of selected papers that appeared in the following periodicals: Journal of Forensic Sciences [www.wileyonlinelibrary.com/journal/jfo] and Forensic Science International [www.elsevier.com/locate/forsciint], Forensic Science International: Digital Investigation [www.elsevier.com/locate/j.fsidi], Forensic Science International: Reports [www.elsevier.com/locate/j.fsir], Science & Justice [www.elsevier.com/locate/j.scijus].

Весомость доказательств авторства с несколькими категориями стилометрических признаков: дискретная модель на основе многочлена [Ishihara S. Weight of Authorship Evidence with Multiple Categories of Stylometric Features: A Multinomial-based Discrete Model. *Science & Justice*. 2023. Vol. 63. No. 2. P. 181–199. https://doi.org/10.1016/j.scijus.2022.12.007]

Аннотация. Исследование эмпирически демонстрирует эффективность двухуровневой многочленной статистической модели Дирихле (многочленной системы) для вычисления коэффициентов правдоподобия (LR) для лингвистических и текстовых доказательств с несколькими стилометрическими типами признаков с дискретными значениями. Коэффициенты правдоподобия рассчитывали отдельно для каждого типа признаков, а именно – для N-грамм слова, символа и части речи (N = 1, 2, 3), которые были объединены в общий коэффициент (LR) посредством слияния логистической регрессии. Производительность многочленной системы сравнивали с производительностью ранее предложенной системы с косинусным расстоянием (косинусная система) с использованием тех же данных (то есть документов, собранных у 2 160 авторов)[1]. Результаты показали, что, во-первых, многочленная система превосходит косинусную систему с объединенными типами признаков по логарифмическому значению коэффициента правдоподобия около 0,01 ~ 0,05 бит; во-вторых, многочленная система эффективнее в работе с более длинными документами, чем косинусная. Хотя косинусная система в целом

[1] Ishihara S. Score-Based Likelihood Ratios for Linguistic Text Evidence With a Bag-of-Words Model = Количественные коэффициенты правдоподобия установления авторства применительно к лингвистическим текстовым доказательствам с использованием модели «набора слов» // Forensic Science International. 2021. Vol. 327. 110980. https://doi.org/10.1016/j.forsciint.2021.110980; Ishihara S., Carne M. Likelihood Ratio Estimation for Authorship Text Evidence: An Empirical Comparison of Score- and Feature-Based Methods = Оценка отношения правдоподобия для текстовых доказательств авторства: эмпирическое сравнение методов, основанных на баллах и признаках // Forensic Science International. 2022. Vol. 334. 111268. https://doi.org/10.1016/j.forsciint.2022.111268.

более устойчива к вариабельности выборки, обусловленной количеством авторов, включенных в справочные и калибровочные базы данных, многочленная система может обеспечить стабильность показателей. Например, значение стандартного отклонения логарифмического значения коэффициента становится ниже 0,01 (10 случайно выбранных авторов для базы данных ссылок и калибровок) при наличии 60 или более авторов в каждой базе данных.

Ключевые слова: *криминалистические текстовые доказательства, коэффициент правдоподобия, двухуровневая многочленная статистическая модель Дирихле, несколько стилометрических типов признаков с дискретными значениями, калибровка и слияние логистической регрессии, показатель логарифмического коэффициента правдоподобия*

Разработка травильной пасты для восстановления серийного номера на алюминиевом блоке двигателя [Uysal S., Yildiz E., Armutcu C., Yalçın Sarıbey A., Uzun L. Development of Etching Paste for Serial Number Restoration on Aluminum Engine Block // Journal of Forensic Sciences. 2023. Vol. 68. No. 4. P. 1325–1329. https://doi.org/10.1111/1556-4029.15303]

Аннотация. Серийные номера двигателей, содержащие информацию об их типе, заводском номере, годе и месте изготовления, используются в целях их идентификации. Такие номера, состоящие из уникальных буквенно-цифровых символов, в случае угона автомобиля, его контрабанды или совершения других подобных преступлений полностью или частично уничтожаются, чтобы скрыть происхождение автотранспортного средства, сделать невозможной идентификацию его владельца. Недостатки современных методов реставрации утраченных номеров, такие как сложность использования химического травления жидкостью на вертикальных поверхностях, ограничения при применении оптических и магнитных методов, а также возможность использования некоторых методов, например таких как дифракция обратного рассеяния электронов, только в лабораторных условиях, обуславливают разработку новых методик.

Целью приведенного исследования, с учетом вышеописанных ограничений и важности восстановления серийных номеров при расследовании уголовных дел, стала разработка травильной пасты, помогающей восстановить стертые символы на блоке двигателя из алюминиевого сплава.

В рамках исследования символы, нанесенные холодным тиснением на блок двигателя, фрезировали на разную глубину, после чего их восстанавливали с использованием травильных паст, изготовленных из различных химикатов и материалов. Результаты экспериментов показали, что травильная паста, приготовленная из 200 мг перлита, 400 мг порошка железа и 450 мкл 20 M NaOH, обеспечила хорошую степень восстановления утраченных номеров. Преимуществами данного метода являются предотвращение чрезмерного травления за счет контроля химической реакции и экономичность. Успешное восстановление номеров на реальном блоке двигателя, простота реставрации на криволинейных поверхностях и возможность использования на месте рассматриваемого события обуславливают перспективность широкого внедрения травильной пасты для восстановления серийных номеров.

Ключевые слова: *алюминий, номер двигателя, травильная паста, облитерация, реставрация*

Идентификация бумаги, из которой изготовлены документы, с помощью гибридного извлечения признаков [Lee J., Kim H., Yook S., Kang T-Y. Identification of Document Paper Using Hybrid Feature Extraction // Journal of Forensic Sciences. 2023. Vol. 68. No. 5. P. 1808–1815. https://doi.org/10.1111/1556-4029.15330]

Аннотация. Подделка документов является серьезной проблемой в Корее, где ежегодно регистрируется около десяти тысяч подобных правонарушений. Исследование бумаги играет решающую роль при изучении документов, подлинность которых вызывает сомнения, например, ценных бумаг или контрактов. Анализ бумаги также может использоваться при расследовании других видов уголовных дел, служа ценным источником криминалистически значимой информации при раскрытии таких преступлений, как, например, шантаж. В процессе производства бумаги создаются различные формовочные метки и образования, которые являются важнейшими признаками ее классификации. Эти характеристики создаются рисунком бумажного полотна и распределением волокон целлюлозы и обнаруживаются при проходящем свете.

Авторы исследования предлагают новый подход к идентификации бумаги, основанный на гибридных признаках. Он объединяет исследование текстур, извлеченных из изображений, преобразованных с применением матрицы совпадений на уровне серого (GLCM) и сверточной нейронной сети (CNN), с другим набором объектов, извлеченных CNN, используя те же изображения в качестве входных данных. Предложенный метод применяли для классификации семи основных марок бумаги, доступных на корейском рынке, с точностью 97,66 %. Результаты подтвердили применимость метода для визуального контроля бумажной продукции и его потенциал при раскрытии уголовных дел, связанных с подделкой документов.

Ключевые слова: *сверточная нейронная сеть (CNN), судебная экспертиза документов, матрица совпадений на уровне серого (GLCM), исследования бумаги, бумажное полотно, исследование спорных документов*

Оценка высококачественных оттисков поддельных штампов, изготовленных на струйных принтерах, с помощью анализа текстуры и коэффициента правдоподобия [Tao Y.-M., Tang H., Yang X., Chen X.-H. Assessment of High-quality Counterfeit Stamp Impressions Generated by Inkjet Printers Via Texture Analysis and Likelihood Ratio // Forensic Science International. 2023. Vol. 344. 111573. https://doi.org/10.1016/j.forsciint.2023.111573]

Аннотация. Исследование высококачественных поддельных оттисков штампов, изготовленных с помощью струйных принтеров, по-прежнему остается сложной задачей для судебной экспертизы документов. Авторами статьи был собран набор данных о различных оттисках штампов, созданных в десяти различных вариантах условий и материалов, а также ручным тиснением.

Было выявлено, что оттиски, выполненные на принтере в режиме высококачественной печати, по своим микроскопическим характеристикам крайне похожи на оттиски, сделанные с помощью ручного тиснения. Эти сходства могут привести к неверным выводам при применении традиционных методов идентификации. В связи с этим был разработан метод идентификации оттисков поддельных штампов по особенностям текстуры и параметрам качества изображения с использованием методов статистического анализа для проверки различий между напечатанными оттисками и оттисками, выполненными ручным тиснением.

Анализ главных компонент (PCA) использовали для демонстрации различий между напечатанными и сделанными вручную оттисками. После фильтрации фона оттисков штампов провели анализ обработки изображений для извлечения признаков матрицы совпадения уровней серого (GLCM), анализ фрактальной текстуры на основе сегментации (SFTA), а также локального бинарного шаблона (LBP) и показателей качества изображения (IQM), которые использовались для выявления характеристик изображений оттисков. Были созданы модели отдельных примеров случайным отбором на основе набора данных об оттисках штампов и система оценки доказательств – оттисков штампов для расчета коэффициентов правдоподобия (LRs) при двух альтернативных гипотезах. С помощью коэффициента правдоподобия интерпретировали откалиброванные оценки как доказательства оттисков штампов. Эти показатели возможно сопоставить с показателями сомнительных доказательств с достаточной достоверностью (частота ошибок = 0,048).

Таким образом, в статье представлена система, позволяющая отличать высококачественные оттиски штампов, напечатанные на принтере, от оттисков, выполненных ручным тиснением, с достаточной степенью достоверности.

Ключевые слова: *исследование спорных документов, обработка изображений, статистический анализ, Байесовская интерпретация, отпечаток штампа*

Судебно-экспертное исследование интернета вещей: анализ мобильного приложения HIKVISION [Dragonas E., Lambrinoudakis C., Kotsis M. IoT Forensics: Analysis of a HIKVISION's Mobile App // Forensic Science International: Digital Investigation. 2023. Vol. 45. 301560. https://doi.org/10.1016/j.fsidi.2023.301560]

Аннотация. Системы видеонаблюдения – это повсеместно распространенные объекты Интернета вещей. Ими можно управлять удаленно с помощью специальных мобильных или компьютерных приложений. HIKVISION – крупный производитель подобных устройств, который предоставляет множество приложений для удаленного доступа к такой продукции. Исследования,

касающиеся цифровой криминалистики систем видеонаблюдения HIKVISION, малочисленны и в настоящее время ограничиваются восстановлением видеоматериалов с самих устройств. При этом практически не затрагиваются элементы, которые могли находиться в данных приложениях и использоваться для доступа к ним. Эти потенциальные источники криминалистически значимой информации в настоящее время не анализируется ни коммерческим программным обеспечением, ни программным обеспечением с открытым исходным кодом, хотя могут содержать важную информацию по ряду следственных вопросов.

В статье анализируется мобильное приложение HIKVISION на операционных системах Android и iOS для исследования содержащихся в них доказательственных данных. Таким образом, авторы внесли свой вклад в продвижение бесплатного программного обеспечения с открытым исходным кодом (FOSS) с целью оказания помощи следователям, в частности для разработки соответствующих анализаторов программного обеспечения ALEAPP и iLEAPP.

Ключевые слова: *судебно-экспертное исследование объектов Интернета вещей, судебно-экспертное исследование мобильных данных, HIKVISION, система видеонаблюдения, com.connect.enduser, com.hikvision.hikconnect, Android, iOS, ALEAPP, iLEAPP*

Я слежу за каждым твоим шагом: судебно-экспертный анализ приложения Tile Tracker [Pace L.R., Salmon L.A., Bowen C.J., Baggili I., Richard G.G. Every Step You Take, I'll be Tracking You: Forensic Analysis of the Tile Tracker Application // Forensic Science International: Digital Investigation. 2023. Vol. 45. St. 30155. https://doi.org/10.1016/j.fsidi.2023.301559]

Аннотация. Рост популярности персональных Bluetooth-трекеров вызвал потребность в разработке инструментов криминалистического и судебно-экспертного анализа, которые помогают правоохранительным органам в установлении различных связанных с ними фактов. По имеющимся данным, на момент написания статьи было продано 40 миллионов устройств Tile Trackers, которые являются одним из самых популярных типов персональных Bluetooth-трекеров. Такой рост применения персональных отслеживающих устройств не прошел бесследно, поскольку участились и сообщения об их использовании для противоправных действий.

Приведенная работа представляет экспертный анализ экосистемы Tile и приложения Tile на iOS, Android и Windows, что позволило выявить ценные для судебной экспертизы источники информации, содержащие разнообразный набор пользовательских данных, включая базы данных SQLite, XML-файлы, файлы кэша и журналы событий, а также координаты геолокации за предыдущие 30 дней. В рамках исследования был разработан инструмент с открытым исходным кодом, способный анализировать подобные криминалистически значимые сведения из приложения Tile: Tile Artifact Parser (TAP). TAP анализирует базы данных SQLite и файлы виртуальной памяти, отображая координаты геолокации и связывая их с временными метками. Возможность быстро и эффективно анализировать и наносить на карту такие метки крайне важна при проведении расследования. TAP также способен обнаруживать и выделять потенциально поддельные данные. Надежность инструмента была протестирована в условиях неполноты или отсутствия данных, что позволило убедиться в его эффективности.

Ключевые слова: *Bluetooth-трекер, Интернет вещей (IoT), судебно-экспертное исследование мобильных устройств, артефакты, судебно-экспертное исследование Android, судебно-экспертное исследование iOS*

AIBFT: набор инструментов для судебной экспертизы браузеров с искусственным интеллектом [Kim H., Kim I., Kim K. AIBFT: Artificial Intelligence Browser Forensic Toolkit // Forensic Science International: Digital Investigation. 2021. Vol. 36. St. 301091. https://doi.org/10.1016/j.fsidi.2020]

Аннотация. В эпоху массового распространения интернет-контента веб-браузеры служат важным связующим звеном между ним и пользователями, иногда выступая при этом источниками распространения вредоносных интернет-вирусов. В последние годы проводятся многочисленные исследования веб-браузеров по выявлению путей заражения различных устройств интернет-вирусами при нарушении протоколов безопасности. Однако общий объем интернет-контента постоянно растет, и по мере повышения производительности сети веб-сайты становятся совершеннее и объемнее, а ко-

личество веб-страниц, доступных в рамках одного отдельно взятого веб-сайта, увеличивается в геометрической прогрессии. Соответственно, в текущих условиях практически невозможно вручную проанализировать подобный объем данных.

В статье предложен метод применения машинного обучения к анализу веб-браузеров для решения обозначенных проблем. Также предлагается использовать набор инструментов для судебной экспертизы браузеров с искусственным интеллектом (AIBFT: Artificial Intelligence Browser Forensic Toolkit), инструмент подтверждения концепции (POC), который обеспечивает автоматическое обнаружение вредоносных веб-страниц с использованием моделей искусственного интеллекта (ИИ), а также проведение анализа вероятности вредоносности ПО и визуализацию временной шкалы. В рамках исследования было изучено 52 500 безопасных и вредоносных веб-страниц для моделирования и обучения ИИ. В результате применения алгоритма случайной выборки (randomforest) среди алгоритмов ИИ была достигнута точность выполнения поставленных задач, равная 99,8 %.

Ключевые слова: *судебно-экспертное исследование браузера с помощью искусственного интеллекта, артефакт, судебно-экспертный инструмент AIBFT на основе искусственного интеллекта*

cRGB_Mem: На стыке судебной экспертизы памяти и машинного обучения [Ali-Gombe A., Sudhakaran S., Vijayakanthan R., Richard G.G. cRGB_Mem: At the Intersection of Memory Forensics and Machine Learning // Forensic Science International: Digital Investigation. 2023. Vol. 45. 301564. https://doi.org/10.1016/j.fsidi.2023.301564].

Аннотация. Вызывающая тревогу проблема усложнения структуры и повсеместного распространения вредоносных программ для мобильных устройств привлекает внимание многих исследователей кибербезопасности. В частности, на платформе Android вредоносные вирусы-трояны, предназначенные для кражи персональных данных пользователей, криптомайнеры, программы-вымогатели и различные схемы мошенничества с использованием пользовательских устройств продолжают распространяться как в рамках магазина приложений Google Store, так и в сторонних магазинах. Несмотря на то, что сообщество, занимающееся изучением подобных вирусов, и индустрия кибербезопасности с 2012 года прилагают большое количество усилий для борьбы с этой угрозой, авторы вредоносных программ постоянно находят способы обойти существующие механизмы обнаружения и предотвращения атак. Во многом такое положение вещей обусловлено ограниченностью набора признаков, используемых при построении классификационных моделей. Таким образом, главной целью статьи является преодоление разрыва между статическим и динамическим анализом путем изучения использования присутствующих в оперативной памяти устройств артефактов, генерируемых в результате использования Android-приложений, для повышения эффективности классификации вредоносных программ. Предлагаемый подход, называемый RGB_Mem, изучает RGB-изображения, сгенерированные на основе моделей распределения оперативной памяти устройств, в сверточной нейронной сети. В результате применения предлагаемого алгоритма классификации была достигнута точность 95,98 % для выборок с известными объектами и 84,48 % – с неизвестными. Эти результаты указывают, что артефакты, восстановленные при проведении экспертизы памяти после ее отключения, могут дать новое направление соответствующим исследованиям, а также материал для обучения, направленного на классификацию вредоносных программ на базе системы Android. Артефакты, восстановленные после выполнения исследования, которым не препятствуют какие-либо ограничения, наложенные на обфускацию (программное обеспечение) и привязку, обеспечивают более точную характеристику приложения и, следовательно, больше подходят для соответствующей классификации.

Ключевые слова: *судебно-экспертное исследование памяти, Android, анализ памяти, вредоносное программное обеспечение, сверточная нейронная сеть, машинное обучение*

Судебно-экспертное исследование объектов промышленного интернета вещей (IIot): забытая концепция в погоне за индустрией 4.0 [Kebande V.R. Industrial Internet of Things (IIoT) Forensics: The Forgotten Concept in the Race Towards Industry 4.0 // Forensic Science International: Reports. 2022. Vol. 5. P. 1–7. https://doi.org/10.1016/j.fsir.2022.100257]

Аннотация. Достижения в области промышленного интернета вещей (IIoT) и усиление его внутренних взаимосвязей, непрерывное развитие интеллектуальных экосистем и автоматизация их процессов при всей своей значимости для человечества расширили спектр потенциальных угроз кибербезопасности. Прежде всего это происходит, когда отрасли стремятся привести свою деятельность в соответствие с требованиями Четвертой промышленной революции (Индустрии 4.0). Стало очевидным, что объединение промышленных операционных технологий (OT) с информационными (IT) приводит к усложнению экосистемы IIoT, смене парадигмы и общим изменениям в архитектурах безопасности и цифровых криминалистических расследований. Следовательно, с расширением зоны его действия, появлением новых и разнообразных моделей поведения систем количество угроз кибербезопасности также постоянно растет. Возможностей для расследования преступлений в сфере IIoT в данный момент недостаточно, поскольку (на момент написания этой статьи) многие отрасли стремятся как можно скорее реализовать цели Индустрии 4.0, не обеспечивая при этом достаточный уровень кибербезопасности. Соответственно, следует признать, что все еще существует недостаточно методологий, стандартов, процессов или моделей зрелости, которые были бы ориентированы на решение криминалистических задач в рамках IIoT. В статье исследуются возможности применения экспертизы IIoT и объясняется необходимость изучения и внедрения в эту сферу криминалистических и судебно-экспертных стандартов и методов. Изложенные в работе предложения могут послужить фундаментом для создания будущих систем расследования, ориентированных на IIoT.

Ключевые слова: *IIoT, кибербезопасность, Индустрия 4.0, цифровой, криминалистика*

Окей, Google, разожги пожар. Устройства Интернета вещей как свидетели и действующие лица при расследовании пожаров [Servida F., Fisher M., Delemont O., Souvignet T.R. Ok Google, Start a Fire. IoT Devices as Witnesses and Actors in Fire Investigations // Forensic Science International. 2023. Vol. 348. 111674. P. 1–11. https://doi.org/10.1016/j.forsciint.2023.111674]

Аннотация. Пожары – одно из самых разрушительных происшествий, с которыми может столкнуться следствие, так как они зачастую очень сильно видоизменяют само место происшествия и уничтожают большинство объектов-носителей криминалистически значимой информации. До сих пор расследования возникновения пожаров в значительной степени основывались на характере горения и систем электропроводки, что позволяло обнаружить возможные источники возгорания, а также на показаниях свидетелей и, с относительно недавнего времени, – на фотографиях очевидцев. По мере распространения устройств Интернета вещей (IoT) различные датчики, встроенные в них, становятся новыми источниками информации об окружающей среде и происходящих в ней событиях. Они собирают и хранят данные в облачных хранилищах или серверах с возможностью удаленного доступа, недоступных для физического воздействия пожара, расширяя информационное поле расследования. В работе представлены исследования двух контролируемых пожаров в квартирах, которые были обставлены мебелью, оснащены устройствами Интернета вещей и подверглись возгоранию. Были изучены сведения, полученные как после осмотра самих объектов после пожара, так и из сопутствующих приложений для смартфонов и облака, и оценена полезность передаваемой ими информации. Это исследование выявило целесообразность учета данных, содержащихся в устройствах Интернета вещей, при расследовании пожаров.

Ключевые слова: *реконструкция пожара, происхождение, причина, цифровая криминалистика, Интернет вещей, умные устройства, умные здания*

Профилирование характерных запаховых следов взрывчатых веществ: обзор последних достижений в области технического анализа и обнаружения [Gallegos Sh.F., Aviles-Rosa E.O., DeChant M.T., Hall N.J., Prada-Tiedemann P.A. Explosive odor Signature Profiling: A Review of Recent Advances in Technical Analysis and Detection // Forensic Science International. 2023. Vol. 347. 111652. P. 1–19. https://doi.org/ 10.1016/j.forsciint.2023.111652]

Аннотация. В условиях постоянно растущей угрозы использования самодельных взрывных устройств (СВУ) и самодельных взрывчатых веществ (ВВ) как внутри стра-

ны, так и за рубежом, обнаружение взрывчатых веществ и связанных с ними материалов является первостепенной задачей при предотвращении террористической деятельности по всему миру. Так, собаки являются наиболее распространенным «биологическим детектором», используемым для обнаружения взрывчатых веществ, благодаря их выдающимся обонятельным способностям, высокой мобильности, эффективному поиску объектов на расстоянии и оптимальной идентификации источников запахов. В то же время существуют устройства, работа которых основана на иных принципах. Важнейшим фактором быстрого обнаружения взрывчатых веществ в полевых условиях является понимание строения ключевых летучих органических соединений (ЛОС), связанных с ними. Технология обнаружения взрывчатых веществ должна охватывать большое число угроз, включая широкий спектр взрывчатых материалов, а также новые химические вещества, используемые при изготовлении самодельных взрывных устройств. В рамках этой важнейшей для национальной безопасности области было проведено несколько исследований, направленных на изучение профиля запаховых следов взрывчатых веществ, изготовленных из различных материалов.

Цель работы – привести базовый обзор этих исследований и краткий инструментальный анализ различных типов, исследованных на сегодняшний день профилей запаховых следов взрывчатых веществ, уделяя особое внимание экспериментальным подходам и лабораторным методам, используемым при химическом анализе паров и смесей взрывчатых веществ. Изучая подобные концепции, можно достичь более глубокого понимания отличительных черт запаховых следов взрывчатых веществ, обеспечивая их улучшенное химическое и биологическое распознавание, а также совершенствуя существующие лабораторные модели, упрощая разработки детекторов взрывчатых веществ разных типов.

Ключевые слова: *профиль запаховых следов взрывчатых веществ, самодельное взрывное устройство (СВУ), самодельное взрывчатое вещество, биологический детектор, электронный детектор, химическая характеристика*

ИНФОРМАЦИЯ О СОСТАВИТЕЛЯХ

Фетисенкова Наталья Викторовна – редактор первой категории информационно-издательского отдела ФБУ РФЦСЭ имени профессора А.Р. Шляхова при Минюсте России;
e-mail: iio@sudexpert.ru

Василевская Дарья Владимировна – переводчик отдела международного сотрудничества ФБУ РФЦСЭ имени профессора А.Р. Шляхова при Минюсте России;
e-mail: iio@sudexpert.ru

CONTRIBUTING EDITORS

Fetisenkova Natal'ya Viktorovna – First Category Editor, Information and Publishing Department, the Shlyakhov RFCFS; e-mail: iio@sudexpert.ru

Vasilevskaya Dar'ya Vladimirovna – Translator, the Department of International Cooperation, the Shlyakhov RFCFS; e-mail: iio@sudexpert.ru