УДК 621.31
Шифр специальности ВАК 2.4.3., 4.3.2.

ОБЗОР ОТДЕЛЬНЫХ ПРАКТИК ВЫЯВЛЕНИЯ НЕЛЕГАЛЬНЫХ МАЙНИНГОВЫХ ФЕРМ

Объем потерь электроэнергии сверх технологического расхода подлежит оплате сетевыми организациями как потери электроэнергии, возникшие в принадлежащих им объектах сетевого хозяйства. Затраты сетевых компаний на компенсацию коммерческих потерь электроэнергии гарантирующим поставщикам не позволяют сетевым компаниям в полном объеме выполнить модернизацию сетей, внедрять высокотехнологичные технические решения для повышения качества электроснабжения [1]. Борьба с коммерческими потерями электроэнергии остается одной из ключевых задач в отрасли, поскольку именно от достоверности объема полезного отпуска электроэнергии зависит обоснованность объемов оказанных услуг по передаче энергии.
Нельзя не обозначить, что значительную часть в общем объеме коммерческих потерь электроэнергии занимает «черный», нелегальный майнинг криптовалют. Развитие майнинговых ферм приводит к сверхпотреблению электроэнергии, так как майнинг является энергоемким процессом. В 2024 г. доказанный ущерб группе компаний «Россети» от действий «черных» майнеров составил более 1,3 млрд рублей. Возбуждено 40 уголовных дел по статьям УК РФ с реальным сроком лишения свободы.
Рассмотрены инновационные решения по выявлению фактов подключения нелегальных майнинговых ферм к энергосетям. Указаны как уже апробированные практически, так и находящиеся в разработке способы и методы.

АВТОРЫ:
В.А. Буторин, д. т. н., профессор,
ORCID ID 0000–0001–6225–4995,
butorin_chgau@list.ru,
ЮУРГАУ, Челябинск, Россия
Е.Н. Клычков,
ORCID ID 0009–0003–2988–5260,
klichkov74@yandex.ru,
Брединский РЭС ПО «МЭС» филиал ПАО «Россети Урал» — «Челябэнерго»

КЛЮЧЕВЫЕ СЛОВА:
#хищения электроэнергии; #нелегальный майнинг; #ИСУЭ; #инновации

↓ ДЛЯ ЦИТИРОВАНИЯ:

Буторин В.А., Клычков Е.Н. Обзор отдельных практик выявления нелегальных майнинговых ферм // Энергия единой сети. 2025. № 5–6. С. 52–63.

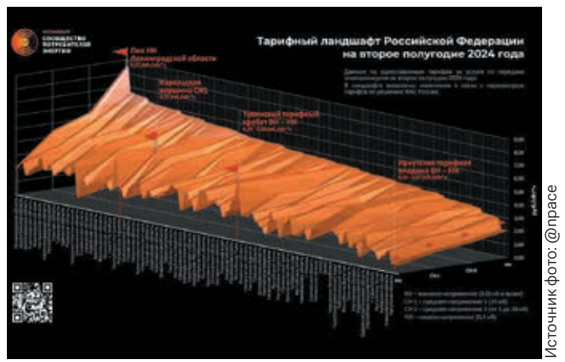
ВВЕДЕНИЕ

По состоянию на апрель 2025 г. майнинг криптовалют официально разрешен в России. По итогам I квартала 2023 г. Россия впервые вышла на второе место в мировом объеме майнинга с общим объемом мощностей, задействованных в создании цифровых валют, 1 ГВт [2]. Деятельность майнеров на территории Российской Федерации с ноября 2024 г. регулируется Федеральным законом от 08.08.2024 № 221-ФЗ. Определены понятия майнинга, пула, адреса кошелька криптовалюты и других элементов, связанных с добычей криптовалюты. Описаны правила работы для майнеров и установлены лица, которые могут майнить. Запрещено совмещение деятельности по майнингу криптовалют с деятельностью по передаче электроэнергии. Согласно [3], с 1 января 2025 г. по 15 марта 2031 г. полностью запрещен майнинг в республиках Северного Кавказа, ЛНР, ДНР, Запорожской и Херсонской областях. Имеется частичное ограничение на работу в зимние периоды для Иркутской области, Забайкалья и Бурятии.

Ситуация для энергосистемы Иркутской области до ввода запрета майнинга была критическая, так как в России наибольшее количество майнинговых ферм приходится именно на этот регион, поскольку там тарифы на электроэнергию ниже, чем в остальных субъектах РФ (рис. 1).

В первом полугодии 2021 г. в Иркутской области электропотребление жилым сектором выросло в полтора раза и составило 4,7 млрд кВт·ч, при этом ни роста населения, ни улучшения благосостояния населения не наблюдалось. Причина — миграция майнинговых ферм после запрета их в Китае. В 2024 г. в Иркутском районе обнаружена незаконная майнинг-ферма, которая нанесла значительный ущерб местной сетевой компании, оцениваемый в 200 млн рублей. [4].

«Россети Северный Кавказ» в 2023 г. выявили 19 случаев неучтенного потребления электроэнергии криптофермами. Объем похищенного энергоресурса равен 22,5 млн кВт·ч [5].



Источник фото: @npacse

Рис. 1. Иркутская тарифная впадина на тарифном ландшафте РФ во втором полугодии 2024 г.

Поиск и локализация очагов коммерческих потерь электроэнергии в районах электрических сетей (РЭС) ПАО «Россети Урал» проводятся в соответствии с разработанным стандартом «Порядок действий при выявлении и устранении причин небалансов электроэнергии в участках сети». Согласно требованиям данного стандарта на начальном этапе работ после формирования баланса пропуска электроэнергии определяются высокопотерьные присоединения ЛЭП 1–20 кВ. В указанных присоединениях по каждой ТП 10/0,4 кВ формируются балансы, проводится анализ потребления электроэнергии юридических и физических лиц. Определяются возможные места хищения электроэнергии по потребителям, имеющим значительное снижение потребления, точки учета с затрудненным доступом для осмотра состояния средств учета, ранее ограниченные по заявкам гарантирующего поставщика электроэнергии, с признаками вмешательства в схему учета согласно данным выгруженных журналов событий с приборов учета интеллектуальных систем учета электроэнергии (ИСУЭ) и т. д. Внедрение ИСУЭ, выполнение полного комплекса работ действительно позволяет значительно сократить временные интервалы на выявление и пресечение фактов хищения электроэнергии [6], но требует определенных навыков работы по аналитике с большим объемом информации для сотрудников служб, групп учета и транспорта электроэнергии (ГТиУЭЭ) [7]. В России продолжает усиливаться кадровый голод в энергетической отрасли. Об этом свидетельствуют данные аналитиков, дефицит специалистов подтверждают и участники рынка [8]. По состоянию на апрель 2025 г. в филиале ПАО «Россети Урал» — «Челябэнерго» 353 вакансии, в основном это мастера, электромонтеры распределительных сетей, электромонтеры ОВБ, техники и инженеры ГТиУЭЭ и др.

Нелегальные майнеры маскируют места размещения ферм, располагая их в хозяйственных постройках, теплицах, подвалах, контейнерах и трудноступной местности.

Скрытность/удаленность размещения нелегальных майнинговых ферм, высокая доля сменяемости персонала в подразделениях РЭС, дефицит квалифицированных, подготовленных сотрудников требуют применения иного подхода к отысканию мест хищений электроэнергии.

СОВРЕМЕННЫЕ СПОСОБЫ ЛОКАЛИЗАЦИИ ОЧАГОВ КОММЕРЧЕСКИХ ПОТЕРЬ ЭЛЕКТРОЭНЕРГИИ

▼ Анализ сетевого трафика

На ПМЭФ-2025 глава компании ПАО «Россети» Андрей Рюмин заявил, что рассчитывает на помощь операторов сотовой связи для выявления нелегальных майнеров [9]. В Китае нашла успешное применение методика выявления майнеров с помощью анализа особенностей сетевого трафика. Для этого производится анализ коммуникационного протокола Stratum.

Stratum — протокол связи, разработанный специально для майнинга криптовалют, таких как биткойн.

Сервер майнингового пула назначает вычислительные задачи подключенным майнерам. Майнеры работают над решением сложной криптографической задачи для создания новой цепи в цепочке блокчейна. Когда найдено действительное решение, оно отправляется обратно в пул для проверки. Если решение принято и соответствует требованиям уровня сложности создателя монет, майнер получает долю от вознаграждения за блок общей цепи криптовалюты [10].

Коммуникационный процесс протокола Stratum имеет такие поведенческие характеристики, как длительное время соединения, небольшой объем данных и частый обмен данными. Эти характеристики значительно отличаются от основных современных основ бизнес/медиа трафика в Интернете.

На первом этапе собираются данные о сетевом трафике, классифицируются, упорядочиваются. Далее каждый поток трафика TCP (Transmission Control Protocol) разбирается по отдельности с анализом TCP-данных для получения статистических характеристик во временных интервалах. Сгенерированный набор данных делится на части и метрики производительности модели классификации случайного леса. Классификация случайного леса (Random Forest) — это алгоритм машинного обучения, который использует ансамбль деревьев решений для предсказания классов объектов (рис. 2).

После сбора необходимых образцов данных их преобразуют из формата PCAP-файлов сетевых пакетов в цифровой формат CSV (рис. 3), который хранит табличные данные в виде обычного текста, и они могут быть легко использованы для анализа, импорта и экспорта данных. Для решения проблемы несбалансированного набора данных используют технику перебора решений. Для передискретизации обрабатываемого массива данных использован алгоритм Borderline-SMOTE. Алгоритм расширяет стратегию выбора точек на опасный, безопасный и шумовой классы. Операции передискретизации выполняются только для точек опасного класса, и выдвигается предположение, что образцы этого типа края могут предоставить более эффективную информацию для модели классификации.

Поскольку в сети отсутствуют данные по майнингу криптовалюты, которые могли бы быть размечены как граничные точки опасного участка выбора точек, необходимо собрать такие данные о трафике, извлечь признаки из собранных данных, извлечь признаки временных рядов из последовательностей трафика, очистить признаки и дождаться считывания алгоритмом обнаружения. После сбора экспериментальных данных и извлечения значений признаков используется алгоритм случайного леса для оценки данных признаков полученного сетевого трафика [11].

Извлечение статистических характеристик временных рядов информации в сетевом трафике и балансировка несбалансированных данных позволяют эффективно определять связь между точками данных, скрытых в сетевом трафике, и выделять зашифрованный сетевой трафик, созданный в результате криптомайнинга, от обычного сетевого трафика.

Анализ сети с помощью PLC-модемов

В ИСУЭ для опроса приборов учета электроэнергии используется технология Power Line Communication (PLC), передача данных по существующим линиям электросетей, по которым осуществляется поставка электроэнергии. Передача данных происходит в высокочастотном диапазоне. Концентратор/маршрутизатор в ходе опроса PLC-модема посылает тестовый высокочастотный сигнал (тон или серию импульсов).

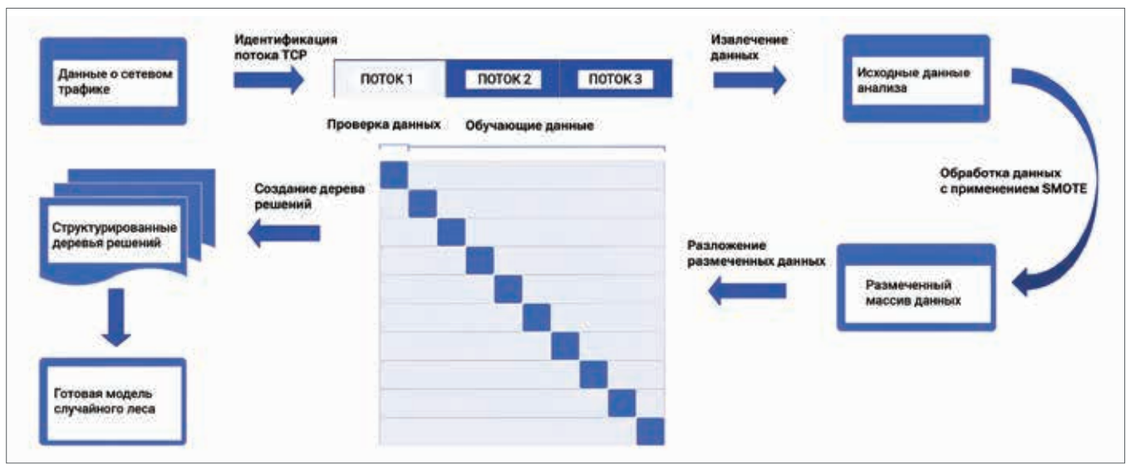


Рис. 2. Общая схема метода идентификации сетевого трафика

Измеряются данные возвращенного сигнала: ослабление сигнала, время ответа, частотные характеристики, фазовый сдвиг и т. п.

Рассмотрим более наглядно на примере шумовых характеристик, как можно локализовать нелегальные фермы. PLC-модем фиксирует, что сигнал от концентратора стал хуже проходить по линии. Частотный отклик канала стал неровным, уровень шума в канале связи вырос на конкретных частотах, аномалия носит стабильный временной характер на суточном графике и повторяется в одно и то же время.

Провалы уровня в канале сигнализируют о нелинейной нагрузке, характерной для импульсных блоков питания майнинговых ферм (рис. 4).

Учеными из Индии в целях обнаружения и мониторинга хищений электроэнергии в сети, имеющей в своем составе PLC-модемы, разработана изобретательная модель Simulink. Simulink — это основанная на MATLAB среда графического программирования для моделирования, симуляции и анализа многодоменных динамических систем. Ее основным интерфейсом являются инструмент для построения графических блок-схем и настраиваемый набор библиотек блоков.

Хищения электроэнергии выявляются и локализуются по изменению амплитуды несущего сигнала в узкой полосе. Отклонение амплитуды передаваемого сигнала отслеживается через регулярные временные интервалы. По изменению амплитуды несущего сигнала можно сделать вывод о наличии подключенной нелегальной фермы [12].

Амплитуда высокочастотного несущего сигнала изменяется из-за меняющегося сопротивления цепи. Импеданс сети меняется при подключении/отключении нагрузок, особенно мощных и нелинейных (например, криптоферм) (рис. 5).

Algorithm 1: feature extraction

Input: A PCAP file
Output: A CSV file containing the features

```
Read the PCAP file;
Create the CSV file;
Initialize flow set S;
foreach packet p in PCAP file do
    if p's FlowId in S then
        if packet has FIN flag then
            Compute the Hurst index of flow based on Equation (1)
              and (2);
            Write all features to CSV file;
            Drop s from S
        else
            Add this packet to flow session;
            Update the statistical features base on updated traffic flow
              session;
    else
        Create a new flow session s;
        Insert s to S;
        Update the statistical features base on new traffic flow session;
```

Рис. 3. Извлечение данных потока TCP в цифровой пакет CSV [11]

Преимущества метода — анализ сети производится на основании данных о поведении и качестве сигнала в линии, а не на характеристиках и величине потребления электроэнергии. Потребители, осуществляющие хищения электроэнергии, подключают нагрузку одинаковой мощности в одинаковые временные интервалы. Алгоритмы машинного обучения позволяют маркировать аномалии передачи сигнала и выявлять с точностью до конкретного прибора учета изменения в передаче несущих сигналов от концентратора/маршрутизатора до PLC-модема.

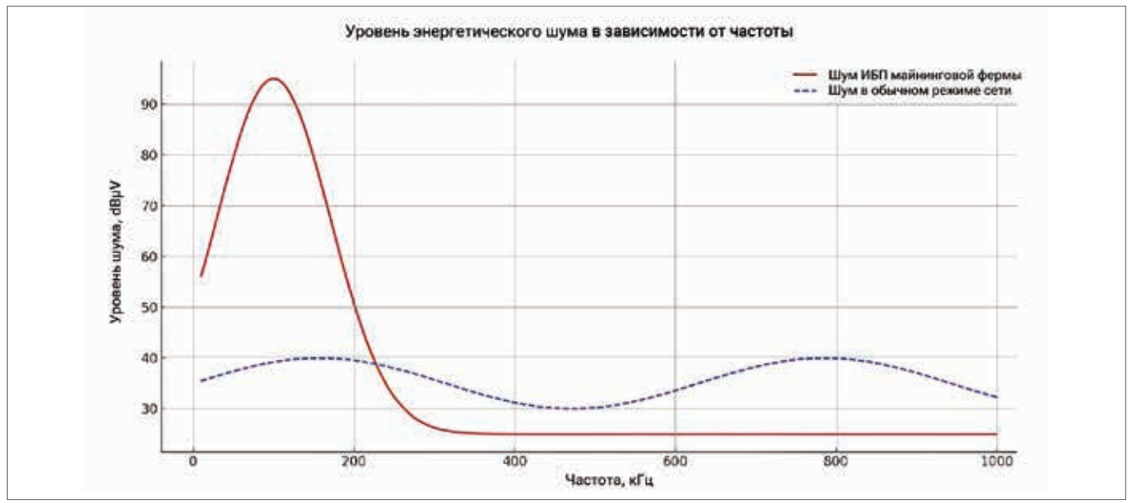


Рис. 4. График зависимости энергетического шума от частоты

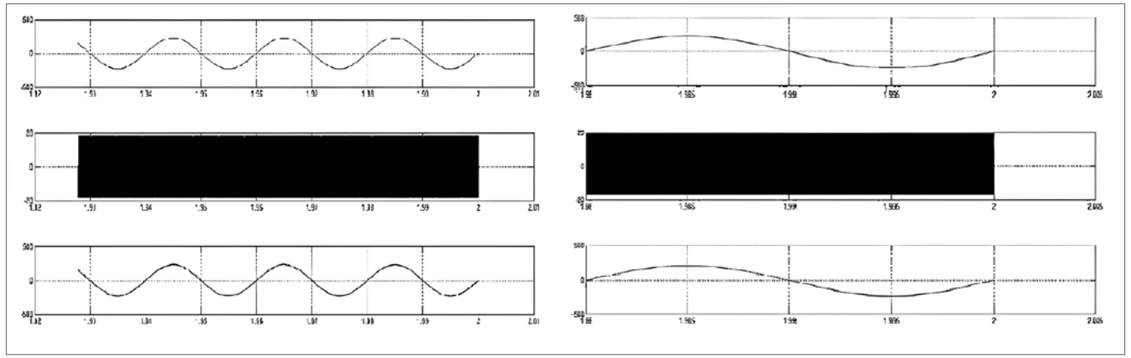


Рис. 5. Осциллограмма амплитуды напряжения в нормальном режиме работы (слева) и в случае включения майнинговой фермы (справа). Ось X – время, с; ось Y — амплитуда напряжения [12]

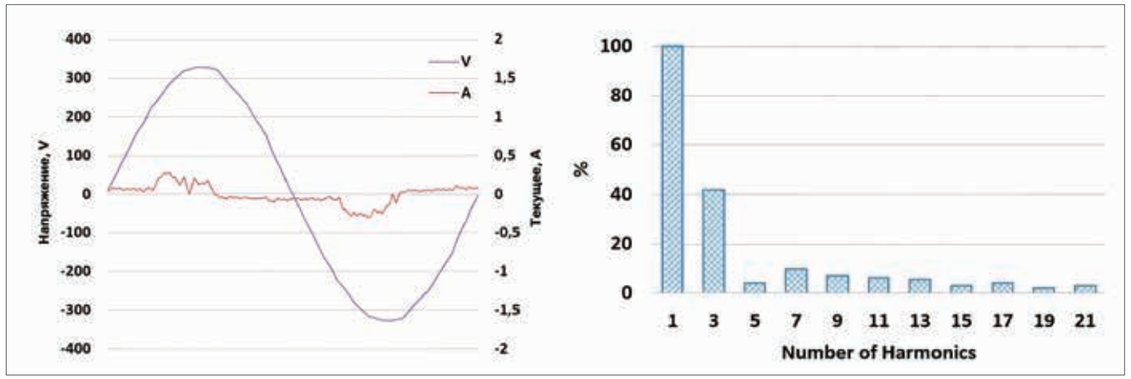


Рис. 6. Напряжение питания, несинусоидальная форма тока и гармонический спектр тока источников питания с переключаемым режимом SMPS [13]

▼ Метод анализа гармонических составляющих

Исследование ученых из Стамбульского университета показало, что выявление нелегальных майнинговых ферм возможно при анализе гармонических составляющих сети. Согласно [13], каждый нелинейный элемент потребляет гармонические токи из сети в различных количествах в зависимости от своих электрических характеристик. Соответственно, если гармонический спектр электрической системы получен, устройства внутри этой системы могут быть обнаружены. Производство криптовалюты осуществляется рядом высокомощных компьютеров. Для питания компьютеров используются источники питания с переключаемым режимом (SMPS). Источники питания с переключаемым режимом потребляют гармонический ток из электрической сети. Из-за того что многочисленные компьютеры, производящие высокие гармонические токи, объединены для производства криптовалют, объекты по производству криптовалют могут быть легко отслежены в распределительной сети через гармонические токи (рис. 6).

Распределительная сеть линейная, ток, протекающий по нейтральной линии, имеет только базовый компонент. Даже если нагрузки идеально сбалансированы в трехфазных четырехпроводных системах с нелинейными нагрузками, такими как источники питания с переключаемым режимом, видеокарты и источники бесперебойного питания (ИБП), нагрузки вызывают токи, протекающие по нейтральной линии, из-за их гармонических токов. Некоторые из гармонических токов ослабляют друг друга, а некоторые полностью компенсируются. Токи третьего порядка увеличиваются в нейтральном проводнике. Гармонические характеристики систем, таких как центры обработки данных и центры производства криптовалюты, которые формируются путем объединения вычислительных компьютеров в ферму, могут быть получены путем изучения уменьшающихся и увеличивающихся значений в гармонических составляющих сети. Наиболее отличительная характеристика электрического тока компьютера возникает в нейтральной линии из-за гармоник третьего порядка (третья, шестая, девятая и т. д.). В местах размещения майнинговых ферм общая мощность оборудования, используемого для производства криптовалюты, несравненно выше, чем у другого оборудования. Поэтому гармоники третьего порядка в нейтральном проводнике могут использоваться в качестве индикатора производства криптовалюты (рис. 7).

Из-за большого количества компьютеров, присутствующих в центрах криптовалют, производственные мощности криптовалют будут генерировать токи, доминируемые гармониками третьего порядка на нейтральной линии. Большое преимущество данного способа выявления майнинговых ферм — это отсутствие требований к наличию и рабочему состоянию ИСУЭ. Необходимо только наличие измерительного оборудования для замера гармонических составляющих в ТП 10/0,4 кВ.

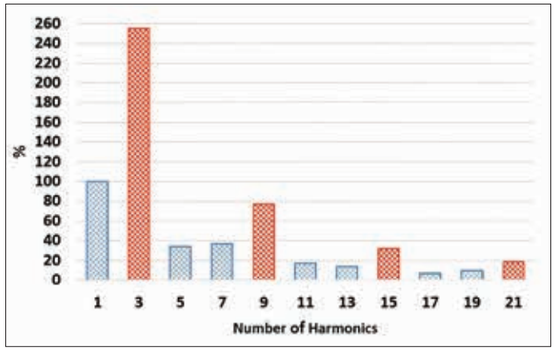


Рис. 7. Значение гармонических составляющих тока нейтрального проводника [13]

▼ Анализ суточных графиков потребления электроэнергии

ПАО «Россети Кубань» реализует алгоритм определения мест размещения майнинговой инфраструктуры на основе ежемесячного анализа электропотребления разных категорий потребителей по статическому характеру нагрузки. Критерии выборки потребителей — среднемесячное потребление в текущем месяце и в течение предыдущих двух лет не опускалось ниже 5000 кВт·ч в месяц. Осуществляются выгрузка и анализ почасовых профилей мощности с приборов учета электроэнергии. Производится анализ дневных/ночных нагрузок, в случае выявления отклонения характера потребляемой мощности от обычной бытовой нагрузки (беспиковое потребление на протяжении всех суток) происходит визуальный осмотр объектов, подключенных от приборов учета, с определением характера и типа подключенной нагрузки (рис. 8) [14]. Контролируются уровень шума, наличие специфического запаха разогретой изоляции и т. п.

Метод применим только для объектов, имеющих подключение через расчетный прибор учета, и преследует цель выявления фактов потребления электроэнергии не для бытовых нужд.

▼ Отслеживание радиочастотного шума

Для обнаружения радиочастотного шума, возникающего от работы майнингового оборудования, можно использовать радиочастотные датчики. Сенсоры электромагнитных помех (EMI-сенсоры) используются для измерения и анализа радиочастотных помех, создаваемых электронным оборудованием, работающим на высокой мощности, таким как майнинговые установки. В процессе работы оборудования (например, серверов, видеокарт, систем охлаждения и преобразователей энергии) возникают радиочастотные помехи, которые могут распространяться через электрическую сеть.

Сенсоры EMI фиксируют изменения в электромагнитном излучении, которое возникает в результате работы высокомощных устройств. Эти изменения могут быть в виде скачков напряжения, высокочастотных колебаний и других аномальных электрических сигналов, характерных для майнинговых ферм. Сенсоры могут быть размещены в низковольтных шкафах ТП 10/0,4 кВ вблизи крупных жилых комплексов и зданий, в распределительных коробках на улицах.

После установки сенсоров и проведения калибровки система сенсоров подключается к централизованной системе мониторинга, которая анализирует данные в реальном времени. Это позволяет автоматически выявлять аномалии и оперативно уведомлять о возможных источниках помех, характерных для работы оборудования криптоферм [15]. Недостатки — ложные срабатывания от иных источников помех.

▼ Поиск теплового следа зданий с помощью общедоступных спутниковых данных

Поскольку майнинг криптовалют отличается высокой вычислительной нагрузкой, значительным энергопотреблением оборудования, требованиями к постоянному охлаждению составляющих криптоферм, высокой локализацией устройств в конкретном месте, разработан метод по отысканию нелегальных майнинговых ферм по тепловым сигнатурам с использованием общедоступных спутниковых данных с тепловым инфракрасным каналом Thermal Infrared, или TIR-каналом.

Специалистами Лаборатории передовых информационных систем (IAAA) Института инженерных исследований Арагона (Испания) предложена методика обнаружения деятельности человека в зданиях в удаленных или труднодоступных районах. Деятельность может быть связана с тепловыми выбросами, которые могут быть обнаружены в том числе в результате анализа спутниковых снимков с наложением теплового следа на карту местности [16].

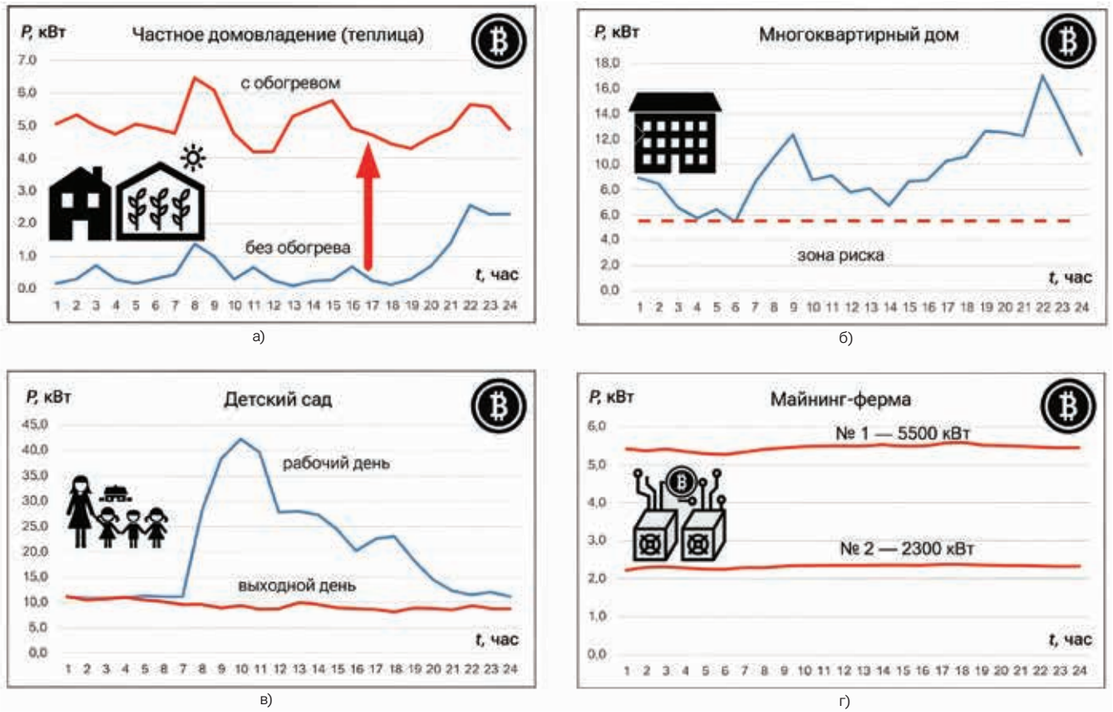


Рис. 8. Суточный график потребления: а) бытовой потребитель с постоянной нагрузкой (теплица/майнинг); б) многоквартирный дом; в) детский сад; г) промышленное предприятие (майнинг) [14]

Ученые сосредоточились на миссии Copernicus Sentinel-2, которая предоставляет частые обновления данных и обнаруживает широкий диапазон частот. Она состоит из двух спутников на полярной орбите, размещенных на одной и той же солнечно-синхронной орбите с временем повторного прохода от двух до пяти дней в зависимости от широты. Изучение производилось по полосе B12. Эта полоса работает в ближнем инфракрасном спектре, а не в диапазоне теплового инфракрасного излучения (8000–14000 нм), который обычно ассоциируется с выбросами тепла человека. В этом исследовании «тепловые сигналы» относятся к паттернам в спектральном ответе полосы B12, которые косвенно указывают на изменения в условиях зданий, такие как человеческая деятельность или использование оборудования.

Ученые обучили четыре модели машинного обучения (XGBoost, LGBM, DNN и CNN), используя изображения с Sentinel-2 B12 и метеорологические данные (температура). Эти модели были обучены на изображениях выборки зданий, полученных от датчиков B12 Sentinel-2, сделанных в разное время, информации о состоянии использования здания на каждом изображении и метеорологических данных с ежедневной температурой в каждой области, использованной для обучения. Модели выводят паттерны активности, которые коррелируют с изменениями в спектральном ответе полосы B12.

В качестве объекта исследовались тепловые сигнатуры четырех сельскохозяйственных ферм в разное время года и с разным присутствием животных в самих помещениях. Производилось сравнение температур воздуха, земли, зданий и т. п. (рис. 9).

Основная цель этого исследования заключалась в том, чтобы изучить возможность использования данных спутника Sentinel-2 для предсказания занятости изолированных зданий в удаленных районах, стремясь обнаружить активность внутри помещений, коррелируя тепловые выбросы с внешними метеорологическими данными, учитывая ограничения общедоступных спутниковых данных и заметное отсутствие специфических датчиков, способных обнаруживать прямые тепловые выбросы изнутри зданий (рис. 10). Данный метод может быть очень эффективным для выявления объектов со значительным тепловым следом в труднодоступной, лесистой или горной местности.

Рис. 9. Определение файлов форм ферм [15]

Блокчейн-аналитика

Все майнеры подключаются к майнинговым пулам по определенным протоколам (наиболее распространенный протокол — Stratum) [10]. Пул агрегирует работу множества майнеров: формирует блоки и распределяет задачи по вычислению уникальных хеш-кодов. После нахождения блока пул распределяет вознаграждение между майнерами через криптокошельки. Как правило, пулы используют один или несколько Collector-кошельков, куда стекаются вознаграждения. На этом кошельке формируются суммы выплат для майнеров. Потом пул делает выплаты участникам (payouts).

Признаками Collector wallet являются:

– большое количество входящих транзакций от разных майнеров/узлов с примерно одинаковыми суммами;
– редкие исходящие транзакции, но крупные — когда кошелек переводит средства на биржи или распределяет по кошелькам участников;
– частое участие в паттерне Common Input Ownership (CIO) с объединением десятков входов.

CIO — это одна из самых распространенных эвристик в блокчейн-аналитике. Она объединяет сотни и тысячи адресов и используется для выявления «кошельковых» кластеров-групп [16]. Так можно идентифицировать биржи, пулы майнеров, сервисы. При выплатах пулам видно характерное объединение адресов. Через определенные промежутки времени пул разом распределяет вознаграждение всем участникам. На блокчейне это проявляется в виде одной транзакции с множеством выходов — хорошо заметный «всплеск» распределений [17]. Отследить данные транзакции позволяют blockchain explorers — сайты, которые дают возможность в реальном времени просматривать блоки, транзакции и адреса [18].

CIO позволяет кластеризировать адреса-реципиенты по метрикам (количество соединений, суммы, повторяемость). Эвристика работает в ~90 % случаев, но не всегда: например, при использовании сервисов-миксеров CIO может дать ложные связи.

Так как все майнеры подключаются к пулам через Stratum, пулы хранят информацию об IP-адресах. Им необходимо отслеживать стабильность соединения, считывать хешрейт по майнерам, вести учет доли каждого участника [19, 20]. Получить реестр IP-адресов можно либо через сотрудничество с пулом, либо через интернет-провайдеров.

В России возможность выявления трафика упрощает «Закон Яровой», который предусматривает использование провайдерами технологии DPI (Deep Packet Inspection) [21]. DPI позволяет провайдеру не просто видеть, куда идет трафик (IP/порт), но и анализировать его содержимое (протоколы, тип данных). Stratum имеет характерный паттерн обмена пакетами, позволяющий DPI выделять его из общего трафика.

При наличии данных о сетевом трафике, объеме и периодичности передаваемых пакетов, а также о частоте и объеме выплат майнерам пулами появляется возможность локализовать майнинговые фермы с привязкой к географической местности.

Если представить процесс в виде схемы, блокчейн-анализ будет выглядеть следующим образом.

1. Из транзакций выплат пула через CIO выявляются группы связанных адресов (например, несколько выплат, объединенных общим владельцем). Это позволяет отделить мелких «домашних» майнеров от промышленных ферм, которые консолидируют доходы. Это необходимо для локализации адресов поиска для провайдеров, так как проверить всех получателей выплат невозможно.
2. На основе выявленных кластеров выплат можно сузить круг потенциальных адресов. Далее с использованием данных пула (при сотрудничестве) или DPI-анализа провайдера возможно локализовать IP-адреса с характерным Stratum-трафиком. Если кластер выплат указывает на крупных получателей,

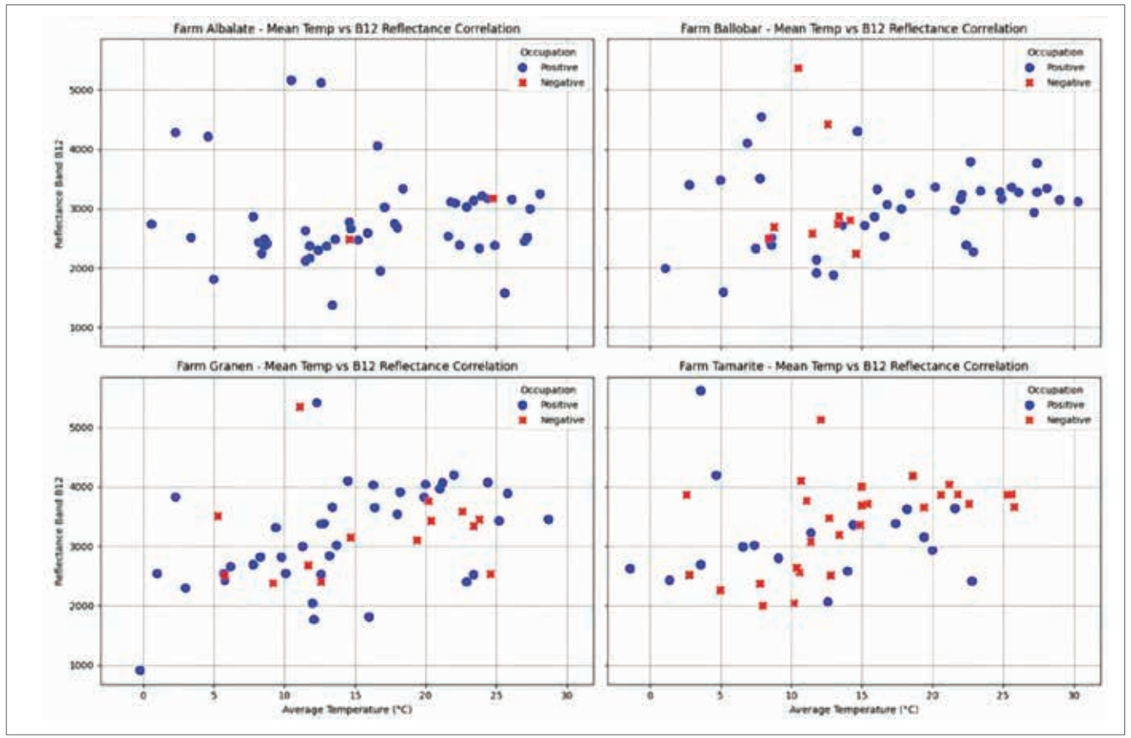


Рис. 10. Корреляция между средней внешней температурой и отражательной способностью в диапазоне B12 на каждой из четырех изученных ферм [15]

эти адреса могут стать целевыми точками для дальнейшего анализа сетевого трафика.

3. После локализации объектов на местности проводится мониторинг характера нагрузки круглосуточно. Если почасовой график нагрузки имеет характерную для майнинговых ферм пологую кривую без типичных для бытовой нагрузки пиков, на основании данных о фактических потерях электроэнергии можно определить очаги нелегального потребления с привязкой к конкретным фидерам ВЛ 10 кВ и ТП 10/0,4 кВ [14].
4. По выявленному реестру возможных мест хищений электроэнергии нелегальными майнерами проводится обследование электроустановок (рис. 11).

▼ Обнаружение термических аномалий с помощью беспилотных летательных аппаратов

Специалистами института фотограмметрии и геоинформации г. Лейбниц (Германия) предложен метод автоматического обнаружения тепловых аномалий.

Как уже указывалось ранее, нелегальные майнеры стараются размещать фермы максимально скрытно: в подвалах, теплицах, контейнерах, нежилых или производственных помещениях, гаражах и т. п. Так как в процессе майнинга образуется значительное количество теплоты, вырабатываемой оборудованием, требуются постоянный отвод и вентиляция помещений с фермами.

Проблему локализации скрытно размещенных ферм можно решить с помощью воздушной тепловой инфракрасной (TIR) съемки на основе ортомозаики, сгенерированной с помощью строгой фотограмметрической обработки. Цель метода — обнаружение температурных аномалий на исследуемом участке поверхности земли.

Температурный след фиксируется как аномалия, если его температура превышает заранее установленный порог. Это достигается путем обнаружения горячих точек в тепловой ортомозаике. Горячие точки ярче, чем окружающая среда на тепловых изображениях, поэтому их можно рассматривать как пятна. Для обнаружения горячих точек в мозаике использован детектор блобов Лапласа — Гаусса.

Детектор блобов Лапласа — Гаусса (Laplacian of Gaussian, LoG) — это метод обнаружения блобов (областей на изображении, где свойства, такие как интенсивность или текстура, однородны или плавно меняются). Он

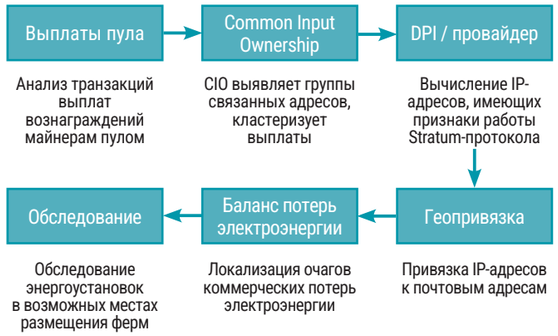


Рис. 11. Схема блокчейн-анализа

В России использование БПЛА также строго регулируется. Для запуска дрона массой свыше 150 г требуется регистрация в Росавиации. Полеты возможны только с разрешения уполномоченных органов и при условии согласования с органами управления воздушным движением. Запрещены полеты вблизи аэропортов, стратегических объектов, в городских зонах без специального допуска. С 2022 г. введены дополнительные ограничения на использование гражданских БПЛА в связи с вопросами безопасности — в большинстве регионов требуется специальное разрешение даже для небольших аппаратов.

В таблице приведены сравнительные характеристики рассматриваемых в статье методов выявления нелегальных майнинговых ферм. Их преимущества, недостатки и применимость на территории Российской Федерации.

ЗАКЛЮЧЕНИЕ

Опыт России и зарубежных стран показывает, что выявление нелегальных майнинговых ферм возможно с использованием различных подходов — от анализа сетевого трафика и блокчейн-операций до применения тепловизоров и БПЛА. Однако многие из этих методов требуют значительных ресурсов, участия операторов связи или применения сложных алгоритмов машинного обучения.

В условиях работы обычных районов электрических сетей ключевое значение приобретают простые и прикладные методы, которые могут быть реализованы силами энергетиков. Наиболее перспективным

сочетает две операции: сглаживание Гаусса и оператор Лапласа (вторая производная). Детектор используется для идентификации и анализа блобов.

Принцип работы в том, что фильтр LoG сильно реагирует на круговые области изображения, где интенсивность резко меняется. Это позволяет обнаруживать блобы разных размеров — регулируя радиус фильтра (масштаб), можно находить блобы разных размеров, а также размечать области, которые выделяются из-за быстрых изменений в свойствах изображения.

Каждый блоб представляется координатами своего центра и соответствующим масштабом, который соответствует масштабу лапласиана (дифференциальный оператор, действующий в линейном пространстве гладких функций). Поскольку эллиптическое представление блоба позволяет лучше локализовать аномалии, впоследствии определяют большую и малую оси эллипса, приспособленного к области пятна. Оси рассчитываются на основе собственных значений и собственных векторов области, полученных из взвешенной матрицы Гессе сглаженного изображения.

На следующем этапе аномалии обнаруживаются на основе найденных горячих точек путем подразделения областей блобов на сегменты с более высокими и более низкими температурами.

В исследованиях использовался беспилотный летательный аппарат (БПЛА) с камерой, оборудованной радиометрическим тепловым имиджером FLIR и оптической камерой для захвата тепловых и визуальных изображений во время полета. Конечным результатом съемки является термографическая ортомозаика интересующего региона [22]. В процессе обнаружения тепловых аномалий неизбежны ложные срабатывания, которые требуют отработки путем обследования по факту уже на местности.

Преимущество метода — возможность обследовать большие по площади массивы частной застройки. Обследование нежилых, производственных огороженных территорий и прочего необходимо проводить, учитывая их соответствие критической инфраструктуре. Съемка может быть расценена как подозрение на разведывательную деятельность.

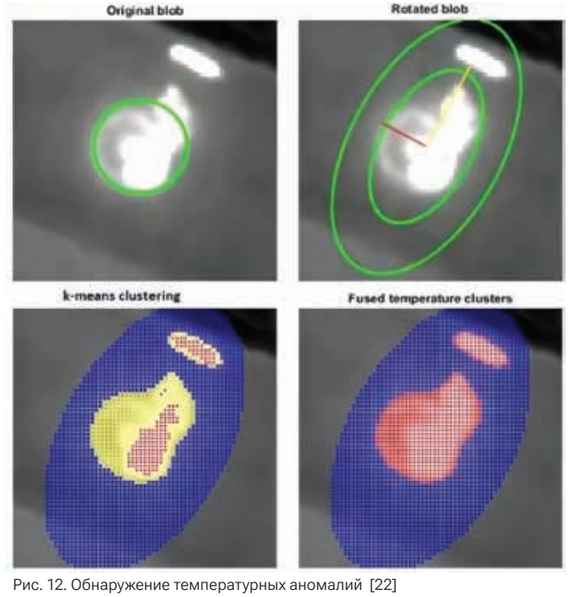


Рис. 12. Обнаружение температурных аномалий [22]

Таблица. Краткая характеристика методов выявления нелегальных майнинговых ферм

Метод	Признак фермы	Трудоемкость выявления	Эффективность	Достоинства	Недостатки	Применимость в РФ
Анализ сетевого трафика (Stratum/DPI)	Характерный паттерн протокола Stratum, длительные соединения, равномерный обмен данными	Высокая (сбор и обработка больших массивов сетевых пакетов)	Высокая при сотрудничестве с провайдерами	Позволяет точечно выявлять фермы, опираясь на уникальные сетевые признаки	Требует доступа к данным операторов связи, вопросы законности	Ограниченно применим (зависит от операторов, но возможен по «Закону Яровой»)
PLC-модемы	Аномалии высокочастотного сигнала, шумы, изменение импеданса	Средняя (данные собираются ИСУЭ, требуется анализ)	Высокая при развитой сети PLC	Локализует до конкретного прибора учета, не зависит от профиля нагрузки	Требует инфраструктуры PLC, уязвим к ложным срабатываниям	Ограниченно, зависит от оснащения ИСУЭ PLC-модемами
Анализ гармонических составляющих	Наличие гармоник третьего порядка в нейтрали, характерных для нелинейных нагрузок	Средняя (нужны замеры на ТП 10/0,4 кВ)	Высокая (отличает майнинговые фермы от бытовых нагрузок)	Не требует ИСУЭ, применим для центров нагрузки	Нужна установка измерительного оборудования	Применим, особенно в распределительных сетях
Анализ графиков нагрузки	Ровный суточный график без пиков, постоянное высокое потребление	Низкая (данные уже собираются приборами учета)	Средняя (хорошо выявляет фермы у бытовых абонентов)	Простая методика, проверена «Россети Кубань»	Не применим при хищениях электроэнергии, помимо учета	Высокая применимость в России
Отслеживание радиочастотного шума (EMI)	Электромагнитные помехи от видеокарт, серверов, БП	Средняя (нужны сенсоры и сеть мониторинга)	Средняя, но с риском ложных срабатываний	Возможность автоматизации и онлайн-мониторинга	Помехи могут создаваться другим оборудованием	Ограниченно применим
Спутниковый анализ тепловых следов (Sentinel-2, TIR)	Тепловые аномалии зданий	Высокая (машинное обучение, корреляция с погодой)	Средняя (низкое пространственное разрешение)	Применим для труднодоступных мест, можно использовать общедоступные данные	Невысокая точность, не различает источники тепла	Ограниченно применим
Блокчейн-аналитика (CIO, выплаты пулов)	Транзакции Collector-кошельков, массовые выплаты	Высокая (нужны алгоритмы кластеризации)	Средняя (обнаруживает кластеры, но не адреса майнеров напрямую)	Позволяет выделить крупных участников для прицельного анализа	Уязвим к CoinJoin/ миксерам	Применим совместно с DPI
ИК-съемка с БПЛА	Тепловые аномалии зданий (горячие точки)	Средняя-высокая (облет, построение ортомозаики)	Высокая (хорошо выявляет скрытые объекты)	Охват больших площадей, подходит для скрытых объектов	Ограничения на полеты, риск нарушить права собственности	Ограниченно применим из-за строгого регулирования БПЛА

в этом плане является анализ гармонических составляющих электрической сети, позволяющий фиксировать характерные признаки работы майнингового оборудования — высокочастотные гармоники в нейтральных проводниках. Данный метод не требует согласования с провайдерами или использования специализированных аналитических платформ, может быть реализован с помощью стандартных измерительных средств на трансформаторных подстанциях.

Таким образом, располагая даже ограниченными ресурсами, энергетические компании могут эффективно выявлять нелегальные майнинговые фермы, минимизируя потери электроэнергии и повышая надежность работы сетей.

Рисунки к статье предоставлены авторами.

↓ ЛИТЕРАТУРА

1. Буторин В.А., Клычков Е.Н. Прогнозирование потерь электроэнергии в АИИС КУЭ как инструмент оптимизации инвестиционных решений компании (на примере Магнитогорских электрических сетей) // Энергия единой сети. 2025. № 3-4 (78). С. 38-48.
2. Электронный ресурс. https://www.forbes.ru/finansy/487282-rossia-vysla-na-vtoroe-mesto-v-mire-po-majningu-kriptovalut. (Дата обращения 30.04.2025).
3. Постановление Правительства Российской Федерации от 23.12.2024 № 1869 «Об установлении запрета на осуществление майнинга цифровой валюты (в том числе участие в майнинг-пуле) в отдельных субъектах Российской Федерации и на отдельных территориях субъектов Российской Федерации».
4. Электронный ресурс. https://www.moneytimes.ru/news/nezakonnaja-maining-ferma/48991/ (Дата обращения 01.05.2025).
5. Электронный ресурс URL. https://www.rossetisk.ru/press_center/company_news/rosseti-severny-kavkaz-presekli-19-faktov-mayning-khishcheniy-elektroenergii-na-bolee-chem-79-mln-r/ (Дата обращения 29.04.2025).
6. Саплин Л.А., Буторин В.А., Клычков Е.Н. Обоснование эффективности внедрения автоматизированных систем контроля и учета энергоресурсов в целях снижения коммерческих потерь электроэнергии // Известия Оренбургского ГАУ. 2024. № 6 (110). С. 186-192.
7. Буторин В.А., Гриценко А.В., Клычков Е.Н. Методика выявления коммерческих потерь электроэнергии // Вестник МЭИ. 2024. № 3. С. 17-24. DOI: 10.24160/1993-6982-2024-3-17-24
8. Электронный ресурс. https://www.kommersant.ru/doc/7180673 (Дата обращения 01.05.2025).
9. Электронный ресурс. https://www.interfax.ru/business/1032413 (Дата обращения 23.06.2025).
10. Электронный ресурс. https://achivx.com/ru/glossary/blok-kandidat/ (Дата обращения 23.06.2025).
11. Dong L., Li Z., Li X., Wang X. & Liu Y. Identification technique of cryptomining behavior based on traffic features // Frontiers in Physics. 2023. № 11. P. 1269889. https://doi.org/10.3389/fphy.2023.1269889
12. Awasthi M., Kumar A., Kumar D. & Pal I. J. Electric power system monitoring and theft detection using power line communication // International Journal of Engineering, Science and Information Technology. 2022. № 2(2). P. 79-85. https://doi.org/10.52088/ijesty.v2i2.254
13. Gül Ö. The Detection of Illicit Cryptocurrency Mining Farms in Electrical Distribution Systems with Innovative Approaches. Preprints. 2021. https:// doi.org/10.20944/preprints202104.0308.v1
14. Богдан В., Попов А., Кизин В. Определение признаков майнинговых деятельности на основании графиков нагрузок // Электроэнергия. Передача и распределение. Ежеквартальный спецвыпуск. 2025. №1 (36). С. 2–8.
15. Zhang G., Ji X., Li Y. & Xu W. Power-based non-intrusive condition monitoring for terminal device in smart grid // Sensors. 2020. № 13. P. 3635. https://doi.org/10.3390/s20133635
16. Suaza-Medina M.E., Lacasta J., López-Pellicer F.J., Béjar R. & Zarazaga-Soria F.J. Detection of changes in the heat emissions signature of buildings related to indoor activity using publicly available satellite data // Earth Science Informatics. 2025. № 18(2). P. 420-435. https://doi.org/10.1007/s12145-025-01926-6
17. Xie H. Bitcoin address clustering method based on multiple heuristic conditions // IET Blockchain. 2022. Vol. 2. Is. 2. P. 89-96. DOI: 10.1049/blc2.12014
18. Электронный ресурс. https://cseweb.ucsd.edu/classes/wi25/cse291-c/lectures/cse291c-wi25-Bitcoin.pdf (Дата обращения 03.09.2025).
19. Yousaf H., Biryukov A., Khovratovich D. Blockchain forensics: survey and open challenges // IEEE Access. 2024. Vol. 12. P. 77621-77645. DOI: 10.1109/ACCESS.2024.11865561
20. Электронный ресурс. https://scispace.com/pdf/detecting-cryptocurrency-miners-with-netflow-ipfix-network-4tz5h7es6m.pdf (Дата обращения 03.09.2025).
21. Федеральный закон от 06.07.2016 № 374-ФЗ «О внесении изменений в Федеральный закон " О противодействии терроризму"...» («Закон Яровой») Электронный ресурс // КонсультантПлюс. http://www.consultant.ru/document/cons_doc_LAW_200839/ (Дата обращения 03.09.2025).
22. Sledz A., Unger J., Heipke C. UAV-based thermal anomaly detection for distributed heating networks // International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences (ISPRS Archives). 2020. Vol. 43. № B1. P. 499-505. DOI: 10.5194/isprs-archives-XLIII-B1-2020-499-2020.