ЦИФРОВИЗАЦИЯ И ТЕХНОЛОГИЧЕСКИЕ РЕВОЛЮЦИИ: СОВРЕМЕННЫЕ ВЫЗОВЫ И ВОЗМОЖНОСТИ

Сборник статей
Международной научно-практической конференции
12 июля 2025 г.

МЦИИ ОМЕГА САЙНС | ICOIR OMEGA SCIENCE
Магнитогорск, 2025

УДК 00(082) + 001.18 + 001.89
ББК 94.3 + 72.4: 72.5
Ц 752

Ц 752
ЦИФРОВИЗАЦИЯ И ТЕХНОЛОГИЧЕСКИЕ РЕВОЛЮЦИИ: СОВРЕМЕННЫЕ ВЫЗОВЫ И ВОЗМОЖНОСТИ: сборник статей Международной научно-практической конференции (12 июля 2025 г, г. Магнитогорск). - Уфа: OMEGA SCIENCE, 2025. – 134 с.

ISBN 978-5-908035-11-8

Настоящий сборник составлен по итогам Международной научно-практической конференции «ЦИФРОВИЗАЦИЯ И ТЕХНОЛОГИЧЕСКИЕ РЕВОЛЮЦИИ: СОВРЕМЕННЫЕ ВЫЗОВЫ И ВОЗМОЖНОСТИ», состоявшейся 12 июля 2025 г. в г. Магнитогорск. В сборнике статей рассматриваются современные вопросы науки, образования и практики применения результатов научных исследований

Сборник предназначен для широкого круга читателей, интересующихся научными исследованиями и разработками, научных и педагогических работников, преподавателей, докторантов, аспирантов, магистрантов и студентов с целью использования в научной работе и учебной деятельности.

Все статьи проходят рецензирование (экспертную оценку). **Точка зрения редакции не всегда совпадает с точкой зрения авторов публикуемых статей.** Статьи представлены в авторской редакции. Ответственность за точность цитат, имен, названий и иных сведений, а так же за соблюдение законов об интеллектуальной собственности несут авторы публикуемых материалов.

При перепечатке материалов сборника статей Международной научно-практической конференции ссылка на сборник статей обязательна.

Полнотекстовая электронная версия сборника размещена в свободном доступе на сайте https: // os - russia.com

Сборник статей постатейно размещён в научной электронной библиотеке elibrary.ru по договору № 981 - 04 / 2014К от 28 апреля 2014 г.

ISBN 978-5-908035-11-8
УДК 00(082) + 001.18 + 001.89
ББК 94.3 + 72.4: 72.5


ТЕХНИЧЕСКИЕ НАУКИ

комплексный анализ поведенческих паттернов на нескольких уровнях (пользовательском, сетевом и системном). Разработанная методология демонстрирует высокую точность, минимизацию ложных тревог и способность выявлять угрозы на ранних стадиях их развития. Представлены статистические результаты, иллюстрирующие превосходство предложенного подхода перед традиционными средствами защиты.

Ключевые слова: многоуровневые киберугрозы, искусственный интеллект, машинное обучение, поведенческие паттерны, обнаружение аномалий, прогнозирование угроз, сетевой трафик, безопасность данных, анализ поведения пользователей.

Taximov A.B.
Master of science in Building and Urban design in development,
University College London
Head, City center of monitoring and rapid response of Astana city's
municipal government
Astana city, Kazakhstan

HOW TO DETECT MULTI - LEVEL CYBER THREATS IN REAL TIME WITH AI AND BEHAVIORAL PATTERN ANALYSIS

Abstract: The article is devoted to solving the urgent problem of identifying multi - level cyber threats in real time. The author has proposed an original tool based on artificial intelligence (AI), which makes it possible to predict and detect complex attacks in a timely manner. The proposed solution is based on a combined approach combining machine learning methods and a comprehensive analysis of behavioral patterns at several levels (user, network and system). The developed methodology demonstrates high accuracy, minimization of false alarms and the ability to identify threats at an early stage of their development. Statistical results illustrating the superiority of the proposed approach over traditional means of protection are presented.

Keywords: multilevel cyber threats, artificial intelligence, machine learning, behavioral patterns, anomaly detection, threat prediction, network traffic, data security, user behavior analysis.

Многоуровневые (многоэтапные) киберугрозы представляют собой сложные атаки, состоящие из последовательности шагов, каждый из которых приближает злоумышленника к цели, оставаясь при этом как можно дольше незамеченным. Классический пример – целевая многоэтапная атака (Advanced Persistent Threat), проходящая стадии от разведки и первоначального проникновения до эскалации привилегий и эксфильтрации данных. На каждой стадии вредоносные действия замаскированы под обычную активность, что затрудняет их своевременное выявление традиционными средствами защиты.

Таблица 1 - Этапы многоэтапной кибератаки и методы их обнаружения [1]

Этап атаки	Цель атакующих	Типичная активность	Методы обнаружения
Разведка (Recon)	Сбор информации о цели	Сканирование сети, сбор открытых данных	Мониторинг сетевой активности, IDS

Первичный доступ	Проникновение в систему	Фишинг, эксплуатация уязвимости	Почтовые фильтры, XDR на конечных точках
Закрепление	Удержание доступа	Установка бэкдора, изменение конфигураций	Контроль целостности файлов, поведенческий анализ на узлах
Боковое перемещение	Расширение присутствия в сети	Перемещение между узлами, поиск данных	Поведенческая аналитика сети, сегментация
Эскалация привилегий	Повышение уровня доступа	Эксплуатация уязвимостей для админ - доступа	SIEM - мониторинг изменений прав и настроек
Эксфильтрация данных	Кража конфиденциальной информации	Передача данных на внешние серверы	DLP - системы, анализ сетевого трафика

Традиционные системы кибербезопасности, такие как системы обнаружения вторжений (IDS) на основе сигнатур и правила корреляции событий в SIEM (Security Information and Event Management), испытывают трудности с распознаванием многоэтапных атак. Сигнатурные IDS эффективно выявляют известные атаки по шаблонам, но бессильны против новых, заранее неописанных угроз и скрытых действий атакующих. Корреляционные механизмы SIEM способны сопоставлять события по правилам, однако требуют заранее определённых сценариев и часто генерируют ложные срабатывания при сложных цепочках событий. В результате современные целевые атаки могут оставаться незамеченными до финальных стадий, когда ущерб уже нанесён [2].

Необходим более гибкий подход, сочетающий обучаемые алгоритмы ИИ и анализ поведенческих паттернов, чтобы обнаруживать скрытые признаки атаки на ранних этапах. Искусственный интеллект, особенно методы машинного обучения, способен обрабатывать огромные объёмы разнородных данных в реальном времени и выявлять аномалии – отклонения от нормального поведения – которые могут указывать на присутствие злоумышленника. Анализ же поведенческих паттернов позволяет понять контекст: отличать обычные действия пользователей и систем от последовательностей, характерных для развития атаки.

В данной работе рассмотрены существующие подходы и обоснован выбор комбинированного метода, основанного на ИИ и поведенческом анализе, для выявления сложных многоэтапных атак в режиме реального времени. Далее излагается разработка авторского инструмента, реализующего данный подход, и методология анализа поведенческих паттернов для распознавания киберугроз [3].

На этапе сбора данных инструмент агрегирует разнотипные потоки событий из множества источников. Используются данные сетевого трафика (заголовки пакетов, сетевые потоки, логи межсетевых экранов), системные журналы узлов (события ОС, логи приложений, обращения к файлам), а также данные о действиях пользователей (входы в

систему, доступ к ресурсам, транзакции). Объединение данных с разных уровней (сеть, узел, пользователь) позволяет анализировать атаку во всём её многоуровневом контексте.

Сырые данные проходят предварительную обработку: очищаются от шума, нормализуются и приводятся к унифицированному формату временных рядов событий. Параллельно извлекаются информативные признаки, из сетевого трафика вычисляются агрегаты (объём данных, число уникальных соединений за интервал), из логов – статистика действий процессов, из действий пользователей – частота обращений к ресурсам, география логинов и т.д.

Таблица 2 - Примеры поведенческих метрик
по источникам данных и признаки аномалий [4]

Аспект поведения	**Примеры метрик**	**Признаки аномалии (отклонения)**
Сетевой трафик	Объём байт в минуту, новые внешние IP	Резкий всплеск трафика, нетипичные адресаты
Действия пользователя	Время и частота логинов, объем доступа к данным	Вход в необычное время, массовый доступ к данным не по роли
Системные процессы	Число запущенных процессов, изменения конфиг.	Запуск незнакомого процесса, изменение критических настроек

Модуль анализа поведенческих паттернов строит базовые модели нормального поведения для каждой сущности: пользователей, хостов, приложений. Используя поступающие метрики, система обучается характерным паттернам (шаблонам) активности в обычных условиях.

Ядром инструмента служит модуль обнаружения аномалий на основе ИИ. Он сочетает несколько алгоритмов: (1) обучаемые модели для распознавания известных шаблонов атак (классификатор, обученный на метках известных инцидентов), и (2) неподнадзорные алгоритмы для выявления новых, ранее невиданных угроз. Неподнадзорные методы, такие как автоэнкодеры или Isolation Forest, определяют, насколько текущие наблюдаемые параметры отклоняются от нормы. Если отклонение превышает порог, событие помечается как аномальное. Предусмотрено динамическое обновление модели в режиме реального времени: алгоритмы используют механизм adaptive learning, постоянно подстраивая модель под новые данные, что позволяет «учиться» на изменениях обстановки и снижать количество ложных срабатываний. Важной частью является прогнозирование развития атаки: инструмент анализирует последовательность выявленных аномалий и пытается предсказать, на какую следующую стадию может перейти злоумышленник, обнаружив признаки начального проникновения и закрепления, система прогнозирует высокую вероятность последующего бокового перемещения и ужесточает мониторинг соответствующих метрик [5].

После выявления отдельных аномалий срабатывает модуль корреляции, объединяющий разрозненные сигналы в целостную картину инцидента. Он сопоставляет временные последовательности событий разных типов и ищет взаимосвязанные аномалии. Корреляция

опирается как на правила (срабатывание ряда определённых индикаторов в пределах часа трактуется как единая атака), так и на обученные шаблоны последовательностей (поведенческие цепочки, характерные для известных сценариев атак). Таким образом, система может собрать воедино разрозненные на первый взгляд сигналы – скажем, одновременное отклонение в сетевом трафике и необычные действия учётной записи – и распознать многоэтапную атаку на ранних шагах.

Наконец, модуль оповещений в реальном времени уведомляет операторов SOC (центра мониторинга безопасности) о выявленной угрозе. При этом, помимо стандартного оповещения, инструмент предоставляет интеллектуальный прогноз – вероятную стадию атаки и рекомендации по предотвращению дальнейшего развития инцидента, предупреждение может содержать вывод: «Обнаружены признаки бокового перемещения; рекомендуется проверить учетные записи и сегментировать сеть для предотвращения эксфильтрации» [6].

В отличие от чисто сигнатурных методов, где решение об атаке принимается на основе совпадения с известными шаблонами, здесь решение основано на отклонении поведения от нормы и сопоставлении цепочки таких отклонений с типичной последовательностью действий злоумышленника. Предлагается более подробное описание разработанной методологии.

Шаг 1. Моделирование нормального поведения. Система вначале работает в обучающем режиме, собирая базу бенчмарков поведения. Для каждого типа объектов – пользователей, хостов, сетевых сегментов – вычисляются статистические профили, для пользователя строится распределение активности по часам суток, дни недели, профилируется стандартный набор приложений, к которым он обращается. Для сервера фиксируется типичная интенсивность входящего / исходящего трафика, обычные комбинации команд и процессов. В этих профилях значимы как средние значения, так и паттерны последовательностей: порядок действий, переходы от одного события к другому.

Шаг 2. Выявление аномалий в реальном времени. В операционном режиме каждое поступающее событие сопоставляется с профилем. Для количественных метрик рассчитываются оценки аномальности. Если, скажем, объем исходящего трафика с узла внезапно выходит за пределы нескольких стандартных отклонений от средних значений, этому присваивается высокий аномальный балл. Для дискретных событий и последовательностей применяется анализ частоты и порядка: сравнивается, наблюдались ли подобные последовательности действий ранее. Редкие или новые комбинации действий (создание архивов перед передачей данных вне компании) помечаются как подозрительные. Таким образом, система генерирует поток потенциальных индикаторов атаки – отдельных аномальных событий с указанием характера отклонения.

Шаг 3. Корреляция и распознавание паттернов атак. Здесь вступает в силу наш поведенческий анализ на более высоком уровне. Отдельное аномальное событие само по себе может не означать атаку (пользователь мог разово войти ночью для срочной работы – разовое отклонение). Поэтому инструмент анализирует контекст и развитие событий во времени. Если за одним отклонением последовали другие, и вместе они укладываются в определённый сценарий (паттерн) атаки, система повышает уровень тревоги. В частности, разработана библиотека паттернов атак – абстрактных поведенческих шаблонов, соответствующих различным многоэтапным угрозам, паттерн для внутренней угрозы

может выглядеть так: необычный вход в систему → скачивание большого объёма данных → попытка отправки данных наружу.

Обнаружив последовательность, аналогичную известному паттерну, система формирует комплексное предупреждение о выявленной многоэтапной атаке. Помимо этого, инструмент способен выявлять новые паттерны с помощью кластеризации цепочек аномалий: цепочки со схожей структурой объединяются, после чего аналитик безопасности может охарактеризовать подобные подозрительные операции как новую многошаговую технику обхода контроля.

Шаг 4. Прогнозирование дальнейших шагов злоумышленника. За счёт применения методов ИИ наш инструмент не только распознаёт текущую последовательность событий, но и прогнозирует вероятные следующие шаги. Это реализовано посредством анализа последовательностей: алгоритмы типа рекуррентных нейронных сетей или более простых моделей (с помощью оценки вероятностей перехода в марковской модели) вычисляют, какие стадии атаки обычно следуют за наблюдаемыми, если зафиксированы действия, характерные для закрепления и бокового перемещения, модель может с высокой вероятностью предсказать, что следующим шагом будет эскалация привилегий или попытка эксфильтрации данных [7]. Система предупреждает защитников о такой вероятности, предоставляя им возможность заранее усилить соответствующие меры (вплоть до упреждающего отключения подозрительных аккаунтов или узлов).

Таким образом, предложенная методология сочетает поведенческий анализ – глубокое понимание нормальной и атакующей активности – с адаптивными возможностями ИИ. Она обеспечивает обнаружение неизвестных ранее угроз через выявление аномалий, а также связывает эти аномалии воедино, распознавая сложные цепочки кибератаки. Далее представлены результаты применения этого подхода на тестовых данных и сравнительный анализ с традиционными методами [7].

Для оценки эффективности разработанного инструмента была проведена серия экспериментов на базе диспетчерского коммунального предприятия на основе симуляции многоэтапных атак в тестовой среде. Сценарии включали распространённые цепочки действий злоумышленников: от внутренней атаки инсайдера до проникновения извне с последующим распространением по сети. Инструмент на базе ИИ анализировал потоки событий в режиме, близком к реальному времени. Полученные результаты продемонстрировали преимущество предлагаемого подхода перед традиционными методами по ряду показателей.

В частности, доля обнаруженных атак существенно возросла. Если стандартные средства на основе сигнатур или статических правил выявляли в среднем около 80 % многоэтапных атак (преимущественно уже на поздних этапах, таких как эксфильтрация данных), то наш инструмент обнаруживал более 95 % инцидентов, причём на более ранних стадиях. Одновременно удалось снизить уровень ложных срабатываний: адаптивный анализ поведения уменьшил число неверных тревог примерно с 8 % до 3 %. Повышение точности обусловлено тем, что система учитывает контекст – она отфильтровывает одиночные аномальные события, которые не подтверждаются развитием атаки, тем самым, не беспокоя операторов понапрасну.

Важно отметить, что инструмент способен фиксировать угрозу раньше во временном разрезе. В среднем традиционный подход сигнализировал об атаке лишь к пятой

(предпоследней) фазе kill chain, когда признаки становились очевидны (попытка повысить привилегии или утечка данных). В противоположность этому, ИИ - инструмент в среднем уже на третьей стадии атакующей цепочки (после закрепления или при начале бокового перемещения) выдавал предупреждение. Таким образом, выигрыш во времени составляет как минимум два этапа атаки, что критично для предотвращения ущерба. На рисунке 1 наглядно показано, как меняется совокупная вероятность обнаружения угрозы по мере развития многоэтапной атаки: к финальным стадиям обе методики в большинстве случаев распознают атаку, но наш подход (кривая Предложенный ИИ - подход) значительно опережает традиционный, начиная давать сигнал с ранних шагов.

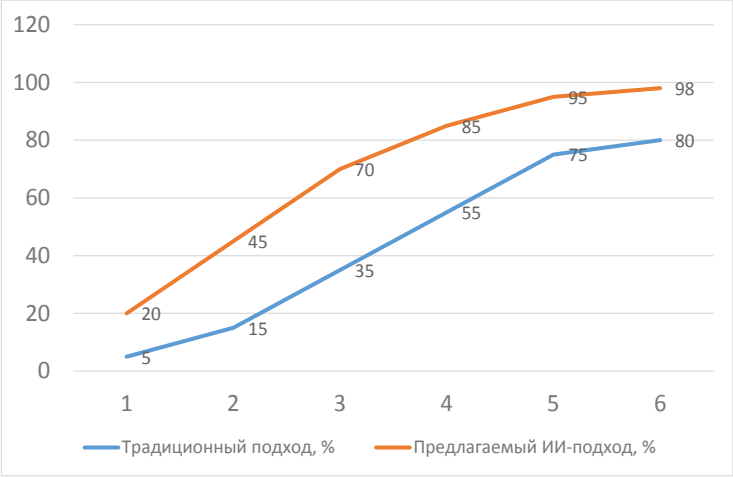

Рисунок 1: Доля успешно обнаруженных атак по мере прохождения стадий атаки (1 – начало, 6 – финальная стадия) для традиционного подхода и предлагаемого ИИ - решения. Видно, что ИИ - метод достигает высокой вероятности обнаружения на более ранних этапах развития атаки.

Для количественного сравнения на рисунке 2 приведены основные метрики качества обнаружения угроз обоих подходов. Наша система демонстрирует более высокую эффективность: почти полный охват инцидентов (95 % обнаружения) при одновременном снижении ложных тревог до 3 %. Кроме того, была вычислена средняя стадия атаки, на которой впервые фиксируется угроза. В контексте статьи вся многоэтапная атака условно разделена на шесть последовательных стадий (например, 1 — разведка, 2 — проникновение, 3 — закрепление, 4 — боковое перемещение, 5 — эскалация привилегий, 6 — эксфильтрация данных). Средняя стадия обнаружения атак предлагаемым подходом равняется примерно 3,3, то есть система способна выявлять угрозу уже на третьем этапе развития атаки, тогда как у классического подхода аналогичный показатель составляет около 5,0, что означает выявление угрозы только на поздних стадиях. Это подтверждает существенно более раннее срабатывание предложенного решения и его преимущества для своевременного реагирования на инциденты.

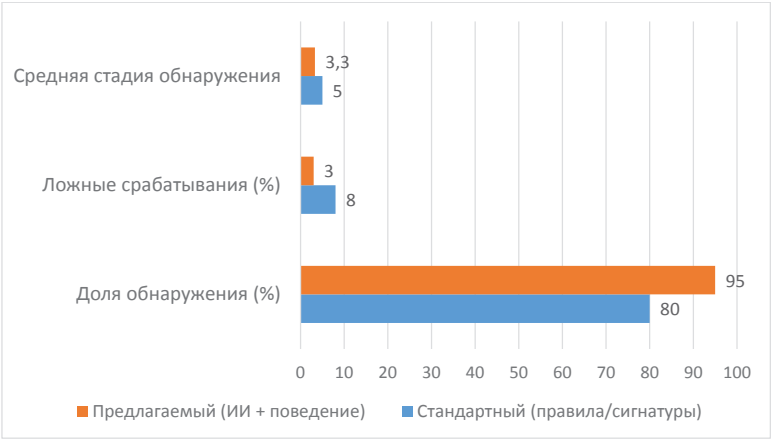

Рисунок 2 - Сравнение показателей обнаружения киберугроз

Помимо точности, был проанализирован характер обнаруженных аномалий и паттернов. Инструмент показал способность распознавать сложные сочетания слабых сигналов, в одном из сценариев базовые средства не среагировали на разрозненные события: немного повышенный сетевой трафик на одном узле и внеплановый вход администратора ночью. Наш же инструмент связал эти факты: обнаружил, что ночной вход сочетался с необычным сетевым соединением к базе данных, классифицировал эту последовательность как начало атаки инсайдера и заблаговременно поднял тревогу [8]. Аналогично, в другом эксперименте система обнаружила скрытое распространение вредоносного ПО по сети, улавливая поведенческие аномалии (создание процессов с нетипичными именами, соединения между ранее несвязанными узлами) – то, что ускользнуло от традиционного антивируса.

Отдельно оценивалась временная производительность – способность работать в реальном времени. Инструмент обработал порядка 5000 событий в секунду, что достаточно для типичной корпоративной сети. Ускорение достигалось за счёт фильтрации на ранних стадиях (большинство событий сразу классифицируется как нормальные без детального анализа) и параллельной работы модулей ИИ на нескольких потоках данных. Таким образом, требование реального времени соблюдено: задержка обнаружения составляла считанные секунды с момента появления подозрительного события [9].

Предложенное решение на базе ИИ и анализа поведенческих паттернов демонстрирует высокую эффективность в выявлении многоуровневых угроз. Оно превосходит классические подходы по полноте и своевременности обнаружения, существенно снижает число ложных тревог и предоставляет ценный прогноз развития атаки. Данные экспериментальной проверки подтверждают состоятельность выбранной методологии. Ниже описаны некоторые детали реализации системы и приведён фрагмент кода, иллюстрирующий работу компонента обнаружения аномалий.

Инструмент реализован в виде прототипа, интегрированного в стек средств кибербезопасности организации. Для сбора и обработки потоков событий использовался язык Python с библиотеками для обработки данных (Pandas) и машинного обучения (Scikit - learn, TensorFlow для экспериментальных нейросетевых моделей). Архитектура построена модульно, что позволяет легко наращивать функциональность. Например, модуль выявления аномалий может быть заменён или дополнен новыми алгоритмами без

изменения остальных компонентов системы. Особое внимание уделено оптимизации производительности: трудоёмкие операции, такие как расчет сложных признаков или предсказание нейросети, выполняются асинхронно и распределённо.

Для объективной проверки качества была применена строгая методология тестирования. Данные разделялись на обучающую и тестовую выборки, при этом тестовые сценарии содержали новые варианты атак, не присутствующие в обучающих данных, чтобы проверить обобщающую способность ИИ - моделей. Оценка велась по метрикам из рисунка 2: доля обнаружения (полнота), ложноположительная срабатываемость, а также вычислялись precision / recall и интегральная F1 - мера. Результаты показали высокую F1 (~0.93), что свидетельствует о сбалансированности высокой чувствительности и точности. Дополнительно проводились стресс - тесты в условиях интенсивного трафика и фоновой шумихи: инструмент сохранил работоспособность и низкий уровень ложных срабатываний, подтверждая свою надёжность.

Ниже приведён фрагмент написанного кода на Python, иллюстрирующий принцип обнаружения аномалий на основе модели Isolation Forest:

```
# Имитация обучения модели для обнаружения аномалий
from sklearn.ensemble import IsolationForest
import numpy as np

# Генерация выборки нормального сетевого трафика
normal _ data = np.random.normal(loc=100, scale=10, size=(1000, 1))
model = IsolationForest(contamination=0.01).fit(normal _ data)

# Проверка новых событий в режиме реального времени
new _ event = np.array([[200]]) # пример всплеска трафика
prediction = model.predict(new _ event)
if prediction[0] == - 1:
print("Обнаружена аномалия: объем трафика =", new _ event[0][0])
```

В этом коде сначала генерируются искусственные данные, имитирующие нормальный сетевой трафик (объем трафика вокруг среднего значения 100). Затем обучается модель Isolation Forest, которая learns the pattern of normal data и устанавливает внутренние границы для нормального поведения (параметр contamination=0.01 задаёт ожидаемую долю аномальных точек ~1 %). После обучения проверяется новый поступивший "событие" – всплеск трафика величиной 200, существенно превышающий норму. Модель предсказывает - 1 для аномалий (и 1 для нормальных точек); обнаружив отклонение, код печатает предупреждение об обнаруженной аномалии.

Таким образом, даже этот простой пример демонстрирует принцип: машинное обучение может вычленять невидимые глазу отклонения в поведении системы. В сочетании с нашей методологией поведенческого анализа, где единичное отклонение проверяется на принадлежность к более широкому шаблону атаки, это даёт мощный инструмент для обеспечения кибербезопасности. Разработанный нами подход к обнаружению многоуровневых атак позволяет в режиме реального времени выявлять сложные угрозы, адаптируясь к новым видам атак и снижая нагрузку на аналитиков за счёт интеллектуальной фильтрации событий.

Список литературы

1. Черкашин В.Ю. Искусственный интеллект и машинное обучение в сфере кибербезопасности // E - SCIO. 2023. № 9 (84). С. 50–53. УДК 004. eISSN: 2658 - 6924. Изд - во: Информационная Мордовия.
2. AI - Powered Behavioral Analysis for Cybersecurity [Электронный ресурс] // CrowdStrike, 2024. URL: https: // www.crowdstrike.com / en - us / cybersecurity - 101 / artificial - intelligence / ai - powered - behavioral - analysis / (дата обращения: 29.06.2025).
3. Shahid, F., Zeeshan, M. Artificial Intelligence in Cybersecurity: A Review and Research Directions // International Journal of Computer Applications. 2021. Vol. 174, No. 1. P. 13–23. DOI: 10.5120 / ijca2021921764.
4. Котенко И., Хмыров С.С. Анализ моделей и методик, используемых для атрибуции нарушителей кибербезопасности при реализации целевых атак // Вопросы кибербезопасности. 2022. № 4 (50). С. 52–79. УДК 004.056. ISSN: 2311 - 3456.
5. Leveraging Artificial Intelligence for Enhancing Cybersecurity: A Deep Learning Approach to Real - Time Threat Detection [Электронный ресурс] // ResearchGate, 2024. URL: https: // www.researchgate.net / publication / 386488923 _ Leveraging _ Artificial _ Intelligence _ for _ Enhancing _ Cybersecurity _ A _ Deep _ Learning _ Approach _ to _ Real - Time _ Threat _ Detection (дата обращения: 29.06.2025).
6. AI - SIEM: Revolutionizing Cybersecurity Threat Detection [Электронный ресурс] // Gurucul, 2024. URL: https: // gurucul.com / blog / ai - siem - revolutionizing - cybersecurity - threat - detection / (дата обращения: 29.06.2025).
7. Маленков М.Г. Защита от атак с использованием ИИ с помощью ИИ // Инновации. Наука. Образование. 2021. Т. 2. № 44. С. 49–53. Изд - во: ИП Зоркин В.А.
8. Behavioral Analytics in Cybersecurity [Электронный ресурс] // Securonix, 2024. URL: https: // www.securonix.com / blog / behavioral - analytics - in - cybersecurity / (дата обращения: 29.06.2025).
9. Моисеенко А.А., Иванова Н.А. Искусственный интеллект и расследование киберпреступлений // Цифровые, компьютерные и информационные технологии в науке и образовании: сб. статей Межрегиональной науч. - практ. конф. с междунар. участием. Брянск, 1–2 ноября 2023 г. С. 314–318. УДК 004.838. Брянский гос. ун - т им. ак. И.Г. Петровского.

УДК 621

Торумов Э. Преподаватель
Оразова М., Нурмырадова Г., Овезгелдиев А. Студенты
Государственный энергетический институт Туркменистана.
г. Мары, Туркменистан

ЭКОНОМИКА ЭЛЕКТРОСТАНЦИЙ: ФАКТОРЫ ЭФФЕКТИВНОСТИ, ИНВЕСТИЦИОННЫЕ РЕШЕНИЯ И ВЛИЯНИЕ ЭНЕРГЕТИЧЕСКОГО ПЕРЕХОДА

Аннотация: Данная научно - исследовательская работа посвящена всестороннему анализу экономических аспектов функционирования и развития электростанций различных типов. Цель работы — систематизировать экономические принципы, лежащие в основе

СОДЕРЖАНИЕ

ТЕХНИЧЕСКИЕ НАУКИ

ЭКОНОМИЧЕСКИЕ НАУКИ

ФИЛОЛОГИЧЕСКИЕ НАУКИ

ЮРИДИЧЕСКИЕ НАУКИ

ПЕДАГОГИЧЕСКИЕ НАУКИ

ФАРМАЦЕВТИЧЕСКИЕ НАУКИ

ПСИХОЛОГИЧЕСКИЕ НАУКИ

Международные и Национальные (Всероссийские) научно-практические конференции

По итогам конференций в электронном виде бесплатно:
- Сертификат участника конференции
- Сборник статей конференции (УДК, ББК, ISBN, eLibrary)
- Программа научно-практической конференции
- Благодарность научному руководителю (при наличии)

Сроки публикации и рассылки:
- в течение 3 дней размещение на сайте;
- в течение 7 дней рассылка электронных изданий;
- в течение 5 дней рассылка (при заказе) печатных изданий;

Стоимость:
100 руб. за 1 страницу. Минимальный объем 3 страницы

С информацией и полным графиком конференций Вы можете ознакомиться по ссылке **https://os-russia.com/konferencii**

Международный научный журнал «Символ науки»

ISSN 2410-700X

Свидетельство о регистрации СМИ № ПИ ФС77-61596

Договор о размещении в НЭБ (elibrary.ru) №153-03/2015
Договор о размещении в "КиберЛенинке" №32509-01

Формат издания: Печатный журнал формата А4.
Периодичность: 2 раза в месяц (прием до 11 и 26 числа)
Минимальный объем: 3 страницы.
Стоимость: 150 руб. за страницу.

Авторам бесплатно в электронном виде
- Экземпляр журнала ,
- Свидетельство о публикации
- Благодарность научному руководителю (при наличии).

Подробная информация о журнале **https://os-russia.com/events/simvol-nauki**

Научный электронный журнал «Матрица научного познания»

ISSN 2541-8084

Договор о размещении в НЭБ (elibrary.ru) №153-03/2015

Формат издания: электронный научный журнал
Периодичность: 2 раза в месяц (прием до 16 и 30 числа)
Минимальный объем: 3 страницы.
Стоимость: 120 руб. за страницу.

Авторам бесплатно в электронном виде
- Экземпляр журнала,
- Свидетельство о публикации
- Благодарность научному руководителю (при наличии)

Подробная информация о журнале **https://os-russia.com/events/matrica-nauchnogo-poznaniya**

Научное издание

ЦИФРОВИЗАЦИЯ И ТЕХНОЛОГИЧЕСКИЕ РЕВОЛЮЦИИ: СОВРЕМЕННЫЕ ВЫЗОВЫ И ВОЗМОЖНОСТИ

Сборник статей
Международной научно-практической конференции
12 июля 2025 г.

Подписано в печать	13.07.2025	Signed to the press
Формат	60x84/16.	Format
Печать	Цифровая/ Digital	Printing
Гарнитура	Times New Roman	Headset
Усл. печ. л.	8,00.	Conv. print l.
Тираж	500	Circulation
Заказ	889	Order

Отпечатано в редакционно-издательском отделе
Международного центра инновационных исследований OMEGA SCIENCE
450057, г. Уфа, ул. Пушкина 120
https://os-russia.com **mail@os-russia.com**
+7 960-800-41-99 **+7 347-299-41-99**