УДК 621.039

Д.Б. КОВАЛЕВ, аспирант гр. АСП-24 СКГМИ(ГТУ)
Научный руководитель Р.В. КЛЮЕВ, д.т.н., проф. СКГМИ(ГТУ)
г. Владикавказ

СИНЕРГИЯ ЦИФРОВЫХ ТЕХНОЛОГИЙ И СИСТЕМ БЕЗОПАСНОСТИ В КОНТЕКСТЕ ТРАНСФОРМАЦИИ ЭЛЕКТРОЭНЕРГЕТИКИ

Аннотация

В работе представлена интеграция современных технологий искусственного интеллекта и кибербезопасности в электроэнергетические системы. Рассматриваются вопросы защиты критической инфраструктуры в условиях децентрализации энергоснабжения и развития Smart Grid. Особое внимание уделяется российским разработкам в области PSIM-платформ и нормативно-правовому регулированию. Представлены практические решения по созданию единых цифровых платформ безопасности для распределенных энергообъектов. Доказана экономическая эффективность внедрения интеллектуальных систем безопасности с показателем снижения капитальных затрат на 25-30%.

Ключевые слова: цифровая трансформация энергетики, безопасность критической инфраструктуры, искусственный интеллект, интернет энергии, умные сети, PSIM-платформы.

В условиях современной геополитической нестабильности и роста гибридных угроз цифровая трансформация топливно-энергетического комплекса (ТЭК) перестала быть вопросом операционной эффективности и стала ключевым элементом национальной безопасности. Такие тренды, как децентрализация генерации на основе возобновляемых источников энергии (ВИЭ) и создание сложных, взаимосвязанных «умных сетей» (Smart Grid), с одной стороны, повышают устойчивость и гибкость системы, а с другой – значительно расширяют поверхность для потенциальных кибератак и диверсионно-террористических актов (ДТА). Новые тактические модели противодействия, применяемые недружественными государствами и внутренними деструктивными элементами, нацелены на стратегически и социально значимые объекты, что делает модернизацию комплексных систем безопасности на основе передовых цифровых технологий не просто актуальной, а жизненно необходимой мерой [1].

В контексте глобальной цифровой трансформации энергетики модернизация систем безопасности становится неотъемлемой частью создания устойчивой инфраструктуры. Современные технологические решения

позволяют интегрировать искусственный интеллект в комплексные системы защиты, что кардинально повышает их аналитические возможности и оперативность реагирования. Особую значимость это приобретает в условиях децентрализации энергоснабжения и распространения возобновляемых источников энергии, где традиционные подходы к безопасности оказываются недостаточно эффективными. Автоматизированные системы на базе ИИ не только минимизируют риски, связанные с человеческим фактором, но и позволяют оптимизировать капитальные затраты за счет рационального использования существующей инфраструктуры технических средств охраны [2,5].

Анализ мирового опыта внедрения искусственного интеллекта (ИИ) в гражданском секторе демонстрирует убедительные результаты в сфере экономической и промышленной безопасности. Согласно исследованию Capgemini, 75% компаний, внедривших системы на базе ИИ для мониторинга активов, отметили значительное повышение безопасности на производственных объектах. Другое исследование, проведенное McKinsey, показало, что использование предиктивной аналитики позволяет предотвращать до 30% инцидентов, связанных с физическими нарушениями, за счет заблаговременного выявления аномальных паттернов поведения. Этот позитивный вектор создает прочную основу для масштабирования подобных решений в энергетике. Интеграция ИИ в единую цифровую платформу энергообъекта позволяет в режиме реального времени анализировать видеопоток, данные с датчиков Интернета Вещей (IoT) и телеметрию технологических процессов, автоматически идентифицируя несанкционированное проникновение, оставленные предметы, отклонения в работе оборудования и кибератаки [3].

Концепция «Интернета Энергии» (IoE), подразумевающая создание единой, самооптимизирующейся и самовосстанавливающейся энергетической сети, является логическим развитием Smart Grid. В контексте безопасности IoE позволяет выстроить многоуровневую систему защиты. В случае попытки ДТА на одном объекте (например, на распределительной подстанции), система не просто локализует угрозу, но и мгновенно перераспределяет потоки энергии через резервные маршруты, минимизируя последствия для потребителей. Технологии блокчейна, применяемые в IoE для заключения smart-контрактов, могут быть адаптированы для обеспечения неизменяемого журнала событий безопасности и управления доступом, что исключает риск внутреннего саботажа. Таким образом, цифровизация через IoE трансформирует энергосистему из набора уязвимых точек в устойчивую, адаптивную и киберустойчивую экосистему, способную парировать как традиционные, так и высокотехнологичные угрозы XXI века.

Перспективным направлением является разработка интегрированных программно-аппаратных комплексов, объединяющих разрозненные подси-

стемы безопасности в единое информационное пространство. Современные платформы демонстрируют способность к агрегации и корреляции разнородных данных от систем контроля доступа, охранно-тревожной сигнализации и видеонаблюдения. Такая интеграция создает основу для реализации предиктивной аналитики, где система не просто фиксирует нарушения, но и прогнозирует потенциальные инциденты на основе анализа паттернов поведения. Эргономичный интерфейс с элементами визуализации предоставляет операторам не просто данные, а готовые сценарии реагирования, что особенно важно при управлении географически распределенными объектами возобновляемой энергетики.

В парадигме Интернета Энергии (Internet of Energy) системы безопасности трансформируются в активный элемент общей цифровой экосистемы. Технологии Интернета Вещей позволяют создавать сети интеллектуальных датчиков, способных в реальном времени отслеживать состояние критической инфраструктуры. Нейросетевые алгоритмы анализируют потоки данных с тысяч устройств, выявляя аномалии и координируя response-мероприятия. Например, при попытке несанкционированного доступа к ветропарку или солнечной электростанции система может автоматически перенаправить энергопотоки, изолировать поврежденный сегмент и уведомить службы безопасности. Такая архитектура соответствует принципам Smart Grid, где безопасность становится не дополнительной опцией, а органичным компонентом управления энергосистемой [6, 8].

Согласно исследованиям Deloitte, внедрение интегрированных систем безопасности с элементами ИИ позволяет сократить количество ложных тревог на 45% и повысить скорость реагирования на инциденты на 60%. При этом капитальные затраты на модернизацию снижаются на 25-30% благодаря возможности поэтапной интеграции новых модулей в существующую инфраструктуру. Дальнейшее развитие связано с созданием межкорпоративных цифровых платформ, где данные о безопасности будут обмениваться между энергокомпаниями в режиме, близком к реальному времени, формируя отраслевой иммунитет к новым вызовам и угрозам.

В условиях текущих геополитических вызовов и санкционных ограничений отечественные разработчики программного обеспечения для систем безопасности демонстрируют активную адаптацию к новым реалиям. Компании-лидеры рынка, такие как «Рубеж», ISS, SoftDivision, TwinPro и Hitech, успешно интегрируют алгоритмы искусственного интеллекта в свои продукты, что особенно актуально для задач цифровизации топливно-энергетического комплекса. Эти решения органично встраиваются в концепцию единой цифровой энергетической платформы, обеспечивая безопасность распределенных объектов генерации на основе возобновляемых источников энергии и элементов умных сетей (Smart Grid).

Ярким примером технологической конвергенции служат PSIM-платформы (Physical Security Information Management), изначально разработанные для управления информацией о физической безопасности. В энергетическом секторе эти системы эволюционируют в инструменты комплексного мониторинга, объединяя данные с датчиков Интернета Вещей (IoT), телеметрию технологического оборудования и видеоаналитику. Такой подход позволяет не только обеспечивать физическую защиту объектов, но и оптимизировать их эксплуатацию в рамках концепции Интернета Энергии (Internet of Energy), где системы безопасности становятся элементом предиктивной аналитики для всего технологического цикла [4].

Регламентация внедрения искусственного интеллекта в системах безопасности осуществляется через профильные нормативно-правовые акты. Государственные корпорации, включая субъекты энергетического сектора, разрабатывают собственные стандарты, устанавливающие требования к функциональности и интеграции интеллектуальных систем. Анализ практики Государственной корпорации по космической деятельности предприятий ракетно-космической отрасли демонстрирует зрелый подход к построению таких регламентов. Среди ключевых документов, определяющих архитектуру комплексных систем безопасности, можно выделить: требования к системам видеонаблюдения с элементами искусственного интеллекта, порядок интеграции систем контроля доступа с аналитическими платформами, использование предиктивной аналитики для оценки угроз безопасности [10].

Эти нормативные акты детализируют требования к алгоритмам компьютерного зрения, протоколам обмена данными между различными подсистемами и процедурам обработки инцидентов с применением ИИ. Опыт предприятий ракетно-космической отрасли представляет значительный интерес для энергетических компаний, поскольку задает высокие стандарты защиты для критически важных объектов инфраструктуры. Адаптация этих подходов к задачам ТЭК позволяет создавать отказоустойчивые системы безопасности, соответствующие как требованиям цифровой трансформации, так и современным вызовам в области защиты стратегических активов.

Выводы:

1. Цифровизация энергетической инфраструктуры требует принципиально новых подходов к безопасности, сочетающих физическую защиту и киберустойчивость в единой архитектуре.
2. Интеграция технологий ИИ и IoT в системы безопасности позволяет не только предотвращать инциденты, но и оптимизировать операционные расходы, демонстрируя снижение капитальных затрат на 25-30%.

3. Российские PSIM-платформы показали свою эффективность для защиты распределенных объектов энергетики, особенно в условиях импортозамещения и санкционных ограничений.

4. Опыт нормативного регулирования предприятий ракетно-космической отрасли в области ИИ может быть успешно адаптирован для энергетического сектора, обеспечивая стандартизацию и безопасность цифровой трансформации.

5. Развитие Интернета Энергии требует создания межкорпоративных платформ обмена данными безопасности, формируя отраслевую систему предиктивного реагирования на угрозы.

6. Дальнейшее развитие связано с интеграцией блокчейн-технологий для обеспечения неизменяемости журналов безопасности и управления доступом к критической инфраструктуре.

Список литературы:

1. Klyuev R.V., Bosikov I.I., Gavrina O.A. Use of wind power stations for energy supply to consumers in mountain territories // Сборник: Proceedings - 2019 International Ural Conference on Electrical Power Engineering, UralCon 2019. – 2019. – С. 116-121.

2. Клюев Р.В., Гаврина О.А., Джиникаев А.О., Икаев А.Э., Теблоев С.К. Использование ветроэлектростанции для электроснабжения потребителей в горных территориях // Энерго- и ресурсосбережение. Энергообеспечение. Нетрадиционные и возобновляемые источники энергии. Материалы Международной научно-практической конференции студентов, аспирантов и молодых ученых, посвященной памяти профессора Данилова Н. И. (1945–2015) – Даниловских чтений. Министерство образования и науки Российской Федерации, Уральский федеральный университет имени первого Президента России Б. Н. Ельцина. – 2017. – С. 756-759.

3. Клюев Р.В., Гаврина О.А., Хетагуров В.Н., Засеев С.Г., Умиров Б.З. Прогнозирование удельного потребления электроэнергии обогатительной фабрики // Горный информационно-аналитический бюллетень (научно-технический журнал). – 2020. – № 11-1. – С. 135-145.

4. Клюев Р.В., Гаврина О.А., Цомаев С.М., Чехоев З.Р. Расчет дистанционной защиты воздушных линий напряжением 110 кВ // Энерго- и ресурсосбережение. Энергообеспечение. Нетрадиционные и возобновляемые источники энергии. Материалы Всероссийской научно-практической конференции студентов, аспирантов и молодых ученых с международным участием. – 2016. – С. 295-298.

5. Вялкова С.А., Моргоева А.Д., Гаврина О.А. Разработка гибридной модели прогнозирования потребления электрической энергии для

горно-металлургического предприятия // Устойчивое развитие горных территорий. – 2022. – Т. 14, № 3 (53). – С. 486-493.

6. Силаев В.И., Гаврина О.А., Голоев Д.Т. Распределенная энергетика труднодоступных территорий на основе плавающих атомных энергоблоков // Электроэнергетика глазами молодежи. материалы XII Международной научно-технической конференции, Нижний Новгород. – 2022. – С. 162-165.

7. Кцоев Х.М., Силаев В.И., Гаврина О.А. Искусственный интеллект в электроэнергетике: методы и технологии // Современные тенденции развития информационных технологий в научных исследованиях и прикладных областях. Сборник докладов II Международной научно-практической конференции, Владикавказ. – 2021. – С. 96-99.

8. Босиков И.И., Клюев Р.В., Гаврина О.А. Анализ геолого-геофизических материалов и качественная оценка перспектив нефтегазоносности южно-харбижинского участка (Северный Кавказ) // Геология и геофизика Юга России. – 2021. – Т. 11, № 1. – С. 6-21.

9. Клюев Р.В., Гаврина О.А., Михальченко С.Н. Анализ удельного потребления электроэнергии обогатительной фабрики // Известия Тульского государственного университета. Науки о Земле. – 2020. – № 1. – С. 433-447.

10. Босиков И.И., Клюев Р.В., Гаврина О.А. Разработка интегрированной системы, включающей алгоритмы и методы анализа надежности промышленно-технической системы // Модели мышления и интеграция информационно-управляющих систем (ММИИУС-2018). Материалы второй Международной научной конференции, посвящённой 25-летнему юбилею Кабардино-Балкарского научного центра Российской академии наук. – 2018. – С. 160-166.

Информация об авторах:

Ковалев Дмитрий Борисович, аспирант гр. АСП-24, СКГМИ(ГТУ), 362021, г. Владикавказ, ул. Николаева, д. 44, shmidt_fridrikh@mail.ru

Клюев Роман Владимирович д.т.н., профессор СКГМИ(ГТУ), 362021, г. Владикавказ, ул. Николаева, д. 44, kluev-roman@rambler.ru.