РОЛЬ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ОБЕСПЕЧЕНИИ КИБЕРБЕЗОПАСНОСТИ ЭНЕРГЕТИЧЕСКИХ ОБЪЕКТОВ

Карабаев Рустам Зафарович
Ташкентский университет информационных технологий, магистрант 2 курса факультета цифровая экономика

Аннотация. *В данной статье рассматривается роль технологий искусственного интеллекта в обеспечении кибербезопасности энергетических объектов. В условиях цифровизации и автоматизации современной энергетической инфраструктуры возрастает количество и сложность киберугроз. В ходе исследования были изучены системы мониторинга на основе искусственного интеллекта, алгоритмы обнаружения угроз и автоматизированные механизмы защиты. Также проанализированы возможности использования искусственного интеллекта в SCADA и промышленных системах управления для раннего выявления кибератак, прогнозирования рисков и повышения устойчивости энергетической инфраструктуры. Результаты исследования показывают, что применение современных цифровых технологий способствует значительному повышению уровня кибербезопасности в энергетическом секторе.*

Ключевые слова: *Искусственный интеллект, кибербезопасность, энергетические объекты, SCADA-система, промышленные системы управления, обнаружение угроз, мониторинг, Smart Grid, автоматизированная защита, критическая инфраструктура.*

ENERGETIKA OBYEKTLARINING KIBERXAVFSIZLIGINI TA’MINLASHDA SUN’IY INTELLEKTNING O‘RNI

Karabayev Rustam Zafarovich
Toshkent axborot texnologiyalari universiteti, Raqamli iqtisodiyot fakulteti yo‘nalishi bo‘yicha 2-kurs magistranti

Annotatsiya*: Ushbu maqolada sun’iy intellekt texnologiyalarining energetika obyektlari kiberxavfsizligini ta’minlashdagi roli tahlil qilingan. Zamonaviy energetika infratuzilmasining raqamlashtirilishi va avtomatlashtirilishi natijasida kiberxavf-xatarlar soni va murakkabligi ortib bormoqda. Tadqiqot davomida sun’iy intellekt asosidagi monitoring tizimlari, tahdidlarni aniqlash algoritmlari hamda avtomatlashtirilgan himoya mexanizmlarining samaradorligi o‘rganildi. Shuningdek, SCADA va sanoat boshqaruv tizimlarida sun’iy intellektdan foydalanish orqali kiberhujumlarni erta aniqlash, xavflarni prognozlash va energetika infratuzilmasining barqarorligini oshirish imkoniyatlari tahlil qilindi. Tadqiqot natijalari energetika sektorida*

zamonaviy raqamli texnologiyalarni qo‘llash kiberxavfsizlik darajasini sezilarli oshirishini ko‘rsatadi.

Kalit so‘zlar: *Sun’iy intellekt, kiberxavfsizlik, energetika obyektlari, SCADA tizimi, sanoat boshqaruv tizimlari, tahdidlarni aniqlash, monitoring, Smart Grid, avtomatlashtirilgan himoya, kritik infratuzilma.*

THE ROLE OF ARTIFICIAL INTELLIGENCE IN ENSURING THE CYBERSECURITY OF ENERGY FACILITIES

Karabaev Rustam Zafarovich
Tashkent University of Information Technologies,
2st year master’s student of the Faculty of Digital Economics

Abstract. *This article examines the role of artificial intelligence technologies in ensuring the cybersecurity of energy facilities. Due to the digitalization and automation of modern energy infrastructure, the number and complexity of cyber threats are continuously increasing. The study investigates AI-based monitoring systems, threat detection algorithms, and automated protection mechanisms. In addition, the possibilities of applying artificial intelligence in SCADA and industrial control systems for early cyberattack detection, risk prediction, and improving the resilience of energy infrastructure are analyzed. The research findings demonstrate that the implementation of modern digital technologies significantly enhances the level of cybersecurity in the energy sector.*

Key words: *Artificial intelligence, cybersecurity, energy facilities, SCADA system, industrial control systems, threat detection, monitoring, Smart Grid, automated protection, critical infrastructure.*

ВВЕДЕНИЕ

В современных условиях цифровизации энергетический сектор является одной из важнейших критических инфраструктур государства. Активное внедрение автоматизированных систем управления, SCADA, ICS и технологий Smart Grid способствует повышению эффективности энергетических объектов, однако одновременно увеличивает количество и сложность киберугроз. Интеграция энергетических систем с интернет-технологиями и цифровыми платформами делает объекты энергетики одной из основных целей для кибератак.

В последние годы кибератаки на энергетические объекты привели к серьезным последствиям, включая перебои в электроснабжении, экономические потери и нарушение функционирования критической инфраструктуры. Особенно уязвимыми являются SCADA и промышленные системы управления, от которых напрямую зависит стабильная работа энергетических предприятий. В связи с этим традиционные методы защиты уже не способны эффективно противостоять современным киберугрозам, что

обусловливает необходимость применения технологий искусственного интеллекта в сфере кибербезопасности.

Технологии искусственного интеллекта позволяют в режиме реального времени анализировать сетевой трафик, выявлять аномалии, прогнозировать возможные угрозы и автоматически реагировать на инциденты. Использование машинного обучения и анализа больших данных значительно повышает эффективность систем защиты энергетической инфраструктуры и способствует снижению вероятности успешной реализации кибератак.

Актуальность данного исследования обусловлена необходимостью изучения возможностей применения искусственного интеллекта для обеспечения кибербезопасности энергетических объектов, оценки эффективности интеллектуальных систем защиты и разработки современных подходов к повышению устойчивости энергетической инфраструктуры.

Гипотеза. Если на энергетических объектах внедрить системы кибербезопасности на основе искусственного интеллекта, включающие интеллектуальный мониторинг, автоматическое обнаружение угроз, технологии машинного обучения и адаптивные механизмы защиты, то уровень киберустойчивости энергетической инфраструктуры значительно повысится, а вероятность успешной реализации кибератак и их негативного воздействия существенно снизится.

Литературный обзор. Проблема применения искусственного интеллекта в обеспечении кибербезопасности энергетических объектов активно исследуется в современной научной литературе. Особое внимание уделяется защите SCADA и ICS-систем, интеллектуальному мониторингу сетевой инфраструктуры и автоматизированному обнаружению киберугроз.

Одним из важных научных источников является Cybersecurity in the Electricity Sector: Managing Critical Infrastructure [1]. В данной работе рассматриваются вопросы управления кибербезопасностью энергетической инфраструктуры, оценки рисков и защиты критически важных систем. Автор Rafal Leszczyna подчеркивает, что современные энергетические объекты требуют комплексного подхода к кибербезопасности, включающего интеллектуальные системы мониторинга и автоматизированный анализ угроз.

Еще одним важным научным источником является Cyber-security of SCADA and Other Industrial Control Systems[2]. В данном исследовании проанализированы уязвимости SCADA-систем и механизмы их защиты. Авторы Edward J. M. Colbert и Alexander Kott отмечают, что нарушения в работе промышленных систем управления могут привести к серьезным сбоям в энергетической инфраструктуре. Исследователи подчеркивают важность применения интеллектуальных алгоритмов обнаружения вторжений и автоматизированных систем защиты.

Существенный вклад в исследование промышленной кибербезопасности внес Eric D. Knapp в книге Industrial Network Security [3]. В работе рассматриваются вопросы

сегментации сетей, мониторинга трафика и выявления аномалий в промышленных системах. Автор отмечает, что технологии искусственного интеллекта позволяют значительно повысить эффективность обнаружения угроз и уровень защиты энергетических объектов.

Практические аспекты применения интеллектуальных технологий киберзащиты представлены в Practical Industrial Cybersecurity [4]. Pascal Ackerman рассматривает возможности использования машинного обучения и автоматизированных систем реагирования на инциденты в энергетическом секторе. Автор также подчеркивает важность повышения квалификации сотрудников энергетических предприятий в области цифровой безопасности.

В исследованиях Eugene Kaspersky [5] рассматриваются современные киберугрозы промышленным объектам, включая вредоносные программы типа Stuxnet. Исследователь отмечает, что применение искусственного интеллекта позволяет повысить эффективность анализа угроз, сократить время реагирования на инциденты и минимизировать риски для энергетической инфраструктуры.

Анализ научной литературы показывает, что использование технологий искусственного интеллекта становится одним из ключевых направлений развития кибербезопасности энергетических объектов. Современные интеллектуальные системы позволяют обеспечить непрерывный мониторинг инфраструктуры, автоматическое обнаружение аномалий, прогнозирование угроз и оперативное реагирование на киберинциденты, что значительно повышает устойчивость энергетического сектора к современным киберугрозам.

Методология исследования. В данном исследовании использовались теоретические, аналитические и сравнительные методы исследования. Основной целью работы являлось изучение роли искусственного интеллекта в обеспечении кибербезопасности энергетических объектов и анализ эффективности интеллектуальных систем защиты.

На первом этапе был проведен анализ научной литературы, международных исследований и нормативных документов в области кибербезопасности энергетической инфраструктуры. Особое внимание уделялось вопросам защиты SCADA и ICS-систем, интеллектуальному мониторингу сетей и технологиям обнаружения киберугроз.

В исследовании применялся метод системного анализа, позволивший определить основные уязвимости энергетических объектов, включая SCADA-системы, удаленные каналы управления и сетевую инфраструктуру. Также был использован сравнительный метод для оценки эффективности традиционных средств защиты и систем на основе искусственного интеллекта.

В рамках исследования анализировались наиболее распространенные типы кибератак на энергетические объекты: DDoS-атаки, вредоносное программное обеспечение, фишинг и атаки на промышленные системы управления. Для каждого

типа угроз оценивались возможные последствия и эффективность интеллектуальных механизмов защиты.

Дополнительно был изучен международный опыт обеспечения кибербезопасности энергетической инфраструктуры, включая анализ известных киберинцидентов в энергетическом секторе. Это позволило определить перспективные направления применения искусственного интеллекта для повышения устойчивости энергетических объектов.

По результатам исследования были разработаны рекомендации по внедрению интеллектуальных систем мониторинга, технологий машинного обучения и автоматизированных механизмов реагирования на инциденты в энергетическом секторе.

Результат исследования. В ходе исследования проведён системный анализ применения технологий искусственного интеллекта в обеспечении кибербезопасности энергетических объектов. Установлено, что цифровизация энергетической инфраструктуры приводит к экспоненциальному росту поверхности атак, особенно в сегментах SCADA/ICS[3], сетевых шлюзах и IoT-устройствах[4]. При этом использование AI-решений позволяет существенно повысить точность обнаружения угроз, снизить время реакции на инциденты и повысить общую киберустойчивость энергетических систем.

Анализ показывает, что ключевым преимуществом AI-систем является переход от сигнатурной модели защиты к поведенческой аналитике. Это позволяет обнаруживать атаки, которые ранее не были известны системе безопасности. Особенно критичным является применение AI в SCADA-системах, где традиционные методы не способны распознавать сложные многоэтапные атаки.

Также установлено, что интеграция AI с SIEM и SOAR платформами позволяет формировать полностью автоматизированный цикл реагирования: обнаружение → анализ → классификация → реагирование → восстановление.

[3] **SCADA** (диспетчерское управление и сбор данных) и **ICS** (промышленные системы управления) - это аппаратные и программные комплексы, которые автоматизируют, отслеживают и контролируют работу промышленных объектов, инфраструктуры и производственных процессов в реальном времени.

[4] IoT (Internet of Things или Интернет вещей) - это концепция сети физических объектов, оснащенных датчиками, программным обеспечением и модулями связи.

Таблица 1

Сравнение классических и ИИ-ориентированных систем кибербезопасности энергетических объектов[5]

№	Параметр оценки	Классические системы защиты	AI/ML ориентированные системы	Научная интерпретация
1	Метод обнаружения угроз	Сигнатурный анализ (rule-based detection)	Поведенческий анализ (behavior analytics)	ИИ выявляет неизвестный угрозы (zero-day)
2	Реакция на инциденты	Постфактум (reactive response)	Реальное время (real-time response)	Снижение времени реакции до минут
3	Обнаружение APT-атак	Низкая эффективность	Высокая эффективность	ИИ анализирует цепочки атак
4	Обработка Big Data	Ограниченная масштабируемость	Высокая масштабируемость	Использование распределенных вычисление
5	Анализ SCADA-трафика	Частичный анализ пакетов	Deep packet inspection совместно с ИИ	Повышение точности анализа процессов
6	Выявление аномалий	Статические правила	ML-анализ отклонений	Обнаружение скрытых атак
7	Устойчивость к модификации атак	Низкая	Высокая	ИИ адаптируется к новым угрозам
8	Уровень автоматизации	20-40%	80-95%	Использование платформ кибербезопасности (SIEM, SOAR)
9	Человеческий фактор	Высокая зависимость	Средняя зависимость	Снижение ошибок человека
10	Предиктивная аналитика	Отсутствует	Реализована	Прогнозирование атак
11	Защита IoT/OT устройств	Ограниченная	Полная модель защиты	Расширение периметра безопасности
12	Стоимость эксплуатации	Средняя	Высокая	Оптимизация затрат в зависимости от ИИ модели

Вышеописанная таблица отражает сравнительный анализ классических и AI-ориентированных систем кибербезопасности, применяемых в энергетических объектах. Её ключевая цель - показать, как изменяется модель защиты при переходе от

[5] Разработано автором в результате исследования

традиционных средств информационной безопасности к интеллектуальным системам, основанным на машинном обучении и анализе больших данных.

С точки зрения функционирования, таблица демонстрирует два принципиально разных подхода:

– Классические системы безопасности работают по сигнатурному принципу. Они заранее «знают» типы атак и реагируют только на уже известные угрозы (например, firewall, IDS/IPS, антивирусные базы).

– AI/ML-системы работают на основе поведенческого анализа (behavioral analytics). Они не зависят от заранее известных сигнатур и могут выявлять аномалии даже в ранее неизвестных типах атак (zero-day угрозы).

В условиях Узбекистана внедрение AI-ориентированных систем кибербезопасности особенно актуально, так как энергетическая отрасль активно модернизируется и проходит этап цифровой трансформации.

1. Электроэнергетические компании и ТЭС.

На тепловых электростанциях (ТЭС) и в распределительных сетях активно используются SCADA-системы для управления производственными процессами. Применение модели из таблицы 1 позволяет:

– выявлять аномалии в работе турбин и датчиков;
– предотвращать несанкционированный доступ к системам управления;
– снижать риск остановки энергоблоков из-за кибератак;
– автоматизировать мониторинг сетевой активности.

2. Диспетчерские центры энергосистем.

В национальной энергосистеме (диспетчерские центры) AI-системы позволяют:

– анализировать большие потоки телеметрических данных в реальном времени;
– выявлять подозрительные изменения в нагрузке сети;
– предотвращать каскадные сбои в энергосистеме;
– повышать устойчивость энергосети при пиковых нагрузках.

Рис.1 Процесс работы и уровни управления ICS системами[6]

Представленное изображение можно интерпретировать как научно-дидактическую схему интеграции Smart Grid, SCADA и ICS в единой архитектуре управления электроэнергетической системой. Визуальная композиция отражает функциональную взаимосвязь между источниками генерации, магистральной передачей электроэнергии, распределительными узлами, центром управления и конечными потребителями, что соответствует современному представлению об интеллектуальной энергетической инфраструктуре.

Содержательно схема демонстрирует многоуровневую организацию энергосистемы. На уровне генерации показаны различные типы источников энергии - биомасса, солнечная, ветровая, атомная, тепловая и гидроэнергетика, что подчёркивает гетерогенный характер производства электроэнергии в условиях Smart Grid. Наличие нескольких источников указывает на необходимость координированного управления, поскольку режимы их работы отличаются по скорости запуска, устойчивости, прогнозируемости и влиянию на нагрузку сети.

Центральное место в схеме занимает Control Center, который следует рассматривать как диспетчерско-управленческий узел, обеспечивающий сбор телеметрических данных, обработку сигналов, мониторинг состояния объектов и выдачу управляющих воздействий. В научном смысле именно здесь реализуются функции SCADA: диспетчеризация, визуализация параметров, сигнализация, архивирование событий и удалённое управление технологическими объектами. Таким образом, SCADA выступает не как самостоятельная физическая инфраструктура, а как программно-аппаратный слой над промышленными объектами управления.

[6] Сгенерировано автором с помощью искусственного интеллекта на основе данных в результате исследования

Правая часть изображения отражает потребительский контур: интеллектуальный город, умные дома, промышленное предприятие и зарядную инфраструктуру для электромобилей. Это демонстрирует расширение традиционной электросети до многосекторной цифровой платформы, в которой нагрузка формируется не только бытовым сектором, но и промышленностью, транспортом и городской инфраструктурой. Следовательно, Smart Grid можно определить как адаптивную электроэнергетическую систему, в которой цифровые технологии обеспечивают динамическое согласование производства, передачи, распределения и потребления энергии.

Стрелочные и линейные связи на изображении отражают два параллельных потока: поток электрической энергии и поток управляющей информации. Первый идёт от источников генерации к потребителям через передающие и распределительные узлы, второй - от сенсоров и полевых устройств к контроллерам, затем к SCADA и центру управления, после чего управляющие команды возвращаются в технологическую среду. Такая двунаправленность является ключевой характеристикой интеллектуальных энергосистем, поскольку именно она обеспечивает адаптивность, отказоустойчивость и оперативное реагирование на изменения режима работы.

С научной точки зрения изображение иллюстрирует трёхуровневую модель:

1. Grid-уровень - физическая энергетическая инфраструктура.
2. ICS-уровень - промышленная автоматизация и контроль оборудования.
3. SCADA-уровень - диспетчерский мониторинг, визуализация и удалённое управление.

Для повышения уровня киберустойчивости энергетических объектов и ускорения цифровой трансформации отрасли предлагается внедрение комплексного подхода, основанного на интеграции технологий искусственного интеллекта, больших данных и автоматизированных систем реагирования. Ключевым направлением является переход от традиционных реактивных моделей к проактивной и предиктивной архитектуре кибербезопасности, где искусственный интеллект выполняет функции непрерывного мониторинга, анализа, прогнозирования и автоматического реагирования на киберинциденты в режиме реального времени.

Особое внимание следует уделить интеграции AI-решений в SCADA/ICS-инфраструктуру энергетических объектов, включая создание централизованных платформ обработки данных, внедрение интеллектуальных SIEM/SOAR систем, развитие цифровых двойников энергетических процессов и использование алгоритмов машинного обучения для анализа аномалий сетевого трафика. Дополнительно важным элементом является развитие кадрового потенциала через внедрение обучающих цифровых платформ с элементами искусственного интеллекта, что позволяет снизить влияние человеческого фактора, являющегося одним из ключевых источников киберрисков.

Также необходимо обеспечить поэтапное внедрение AI-технологий с учетом уровня цифровой зрелости энергетических предприятий, начиная с систем мониторинга и заканчивая полностью автоматизированными системами киберзащиты, способными самостоятельно принимать решения по блокировке угроз и восстановлению нормального функционирования инфраструктуры.

Заключение и выводы. В ходе проведённого исследования была рассмотрена роль искусственного интеллекта в обеспечении кибербезопасности энергетических объектов, а также проанализированы современные угрозы, характерные для цифровизируемой энергетической инфраструктуры. Особое внимание было уделено SCADA/ICS-системам, промышленным сетям и объектам критической инфраструктуры, которые в условиях цифровой трансформации становятся основными целями кибератак.

Анализ научной литературы и практических кейсов показал, что традиционные методы защиты (сигнатурные системы, классические firewall и IDS/IPS) уже не обеспечивают достаточного уровня устойчивости к современным сложным и многоэтапным атакам, включая APT-атаки и zero-day угрозы. В этих условиях искусственный интеллект становится ключевым инструментом перехода от реактивной модели безопасности к проактивной и предиктивной системе защиты.

Результаты исследования подтверждают, что AI-технологии, основанные на машинном обучении, анализе больших данных и поведенческой аналитике, позволяют значительно повысить эффективность обнаружения угроз, сократить время реагирования на инциденты и снизить вероятность успешных кибератак на энергетическую инфраструктуру. Наиболее эффективными направлениями применения ИИ являются интеллектуальный мониторинг сетевого трафика, анализ аномалий в SCADA-системах, прогнозирование атак и автоматизация реагирования через SIEM/SOAR-платформы.

Отдельно следует отметить, что внедрение искусственного интеллекта оказывает не только технический, но и организационный эффект, снижая зависимость от человеческого фактора и повышая общий уровень киберграмотности персонала энергетических предприятий. Важную роль также играет интеграция образовательных цифровых платформ, направленных на подготовку специалистов в области кибербезопасности.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ:

1. Stallings W. Network Security Essentials: Applications and Standards. Pearson Education, 2017.

2. Knowles W., Prince D., Hutchison D. A Survey of Cyber Security Management in Industrial Control Systems. International Journal of Critical Infrastructure Protection, 2015.

3. Knapp E.D., Langill J.T. Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems. Syngress, 2014.

4. Ackerman P. Industrial Cybersecurity: Efficiently Secure Critical Infrastructure Systems. Packt Publishing, 2021.

5. Humayed A., Lin J., Li F., Luo B. Cyber-Physical Systems Security - A Survey. IEEE Internet of Things Journal, 2017.

6. Столлингс В. Основы сетевой безопасности: приложения и стандарты. - М.: Вильямс, 2019.

7. Козырев А. Ю. Информационная безопасность критически важных объектов инфраструктуры. - М.: Горячая линия - Телеком, 2020.

8. Шаньгин В. Ф. Защита информации в компьютерных системах и сетях. - М.: ДМК Пресс, 2018.

9. Иванов А. В., Петров С. Н. Промышленные системы управления и кибербезопасность SCADA/ICS. - СПб.: БХВ-Петербург, 2021.