УДК 621.311: 004.056

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ЭЛЕКТРОЭНЕРГЕТИКЕ

К.Б. Корнеев[1], В.К. Корнеев[2]
[1]Тверской государственный технический университет (г. Тверь),
[2]Национальный исследовательский технологический университет «МИСИС» (г. Москва)

Аннотация. Увеличение использования информационных технологий в промышленном секторе и, что наиболее важно, в таком критически важном направлении, как энергетика, приводит к необходимости построения систем контроля потоков информации, собираемой, передаваемой и обрабатываемой на предприятиях отрасли. При этом перенос хранения и обработки информации в «облако», с одной стороны, повышает надежность и скорость обработки информации, а с другой – делает систему более уязвимой для внешнего нелегитимного воздействия. Интеграция высокосвязанных элементов сети «интернета вещей» (IoT) также может негативно повлиять на защищенность информации.

Ключевые слова: электроэнергетика, информационная безопасность, кибератака, киберпреступления, надежность.

DOI: 10.46573/2658-7459-2026-1-50-58

Спрос на более активное управление энергией и более доступное энергоснабжение способствовал быстрому росту распределенной генерации у потребителей. Тем самым клиенты получили доступ к более сложным энергетическим продуктам, наделенным интеллектуальными технологиями и алгоритмами для удаленного и автономного управления спросом на энергию. Генерирующим активам необходимо максимально использовать присущую им гибкость в изменении мощности, которая потенциально приносит пользу всей системе, сохраняя при этом стабильность на всех ее уровнях. В последнее время все больше внимания уделяется цифровым функциям управления, таким как искусственный интеллект (ИИ) и аналитика. Эти интеллектуальные элементы способствуют обеспечению баланса мощности в режиме реального времени, проводя мониторинг и контроль с высокой степенью детализации и точности. Заинтересованные стороны в локальных системах Smart-Grid («умной сети») могут получить выгоду от возможности локального управления по той причине, что может быть достигнута автономная и локально самодостаточная энергетическая система.

Однако интенсивный обмен информацией между интеллектуальными элементами может привести к серьезной проблеме безопасности из-за конкурирующих интересов различных пользователей или заинтересованных сторон, высокого уровня взаимозависимости, а также в силу своей социальной и технической сложности. В таком взаимодействии сталкиваются интересы двух сторон, где генерирующая компания стремится к максимально точному учету отпущенной энергии, а потребитель старается заплатить минимальную цену за потребленную энергию, что порой ведет к применению противозаконных методов воздействия на системы учета и управления [1]. Во

взаимодействии могут также участвовать сторонние силы, которые имеют деструктивные намерения, направленные на снижение надежности функционирования энергосистемы [2].

В целом существует две категории угроз, связанных с обработкой информации в энергосетях: эксплуатационные угрозы и информационные угрозы. Выделяют три типа эксплуатационных угроз – манипулирование данными, выдачу себя за другое лицо и отказ в обслуживании (DoS). Вторая категория угроз – это угроза раскрытия конфиденциальной информации. Интеллектуальные элементы неизбежно увеличат и без того значительный обмен данными, поднимая требования к конфиденциальности и неразглашению информации на чрезвычайно высокий уровень [4–6]. Хотя больше внимания уделяется именно этой области, все еще отсутствует понимание цифрового перехода энергетической системы и методики работы с большими данными. Современная диспетчеризация очень сильно зависит от точных измерений, а также интерактивного управления через интеллектуальные элементы. Анализ на основе больших данных помогает в поддержке принятия решений, а также автоматизирует процесс управления оперативными переключениями; кроме того, на основе этого анализа может осуществляться стратегическое планирование во многих службах энергопредприятий. Таким образом, целостность данных имеет первостепенное значение для адекватности управления энергосистемой [7].

Как правило, основная часть атак на объекты энергосистемы и жилищно-коммунального хозяйства направлена на ограничение функциональности по причине значительно большего экономического эффекта, производимого неработоспособностью систем, по сравнению с косвенными репутационными потерями. Тем не менее в последние годы с увеличением экономического влияния биржевых показателей на инвестиционные и эксплуатационные показатели работы энергокомпаний негативная информация о доступе к данным может значительно сказаться на финансовых показателях и показателях реализации проектов. По этой причине защита данных от кибератак становится одним из приоритетных направлений работы отделов информатизации и безопасности предприятий.

Согласно современному подходу [8], кибератакам подвергается целостность общей информации, конфиденциальность данных и доступность обслуживания. Эти три типа кибератак частично пересекаются, а частично входят в ранее обозначенные типы эксплуатационных и информационных угроз. В зависимости от цели выделяют четыре основные категории кибератак: на доступность сети, на конфиденциальность, на устройство и на данные. Для проникновения и захвата контроля над информационными системами и системами управления злонамеренное вмешательство обычно использует четыре метода – сканирование, эксплуатацию, разведку и поддержание доступа. В случае энергосистем по причине большой территории покрытия, а также сложной иерархии взаимодействия многие из воздействий могут долгое время оставаться невыявленными, что приводит к инцидентам, становящимся впоследствии достоянием общественности. В силу того, что при этом страдает критическая инфраструктура, сведения об инцидентах могут быть отрывочными, противоречивыми, а также, в зависимости от стороны инцидента, преследовать особые политические или экономические цели. Как правило, первоначальные публикации связаны с жалобами рядовых потребителей сервисов на недоступность или ограниченную функциональность, и только спустя некоторое время возможно разглашение сведений о причинах, а также оценка последствий. В таблице приведены наиболее значимые инциденты, повлекшие за собой значительное возрастание

риска для жизни и здоровья населения, а также приведшие к массовому недоотпуску электроэнергии.

Инциденты в электрических сетях и на электроэнергетических предприятиях, вызванные злонамеренным воздействием на информационную инфраструктуру

Инцидент	**Месяц, год**	**Описание события**
1	2	3
Отключение АЭС Дэвис-Бесс, США	Январь, 2003	Во время проведения обслуживания АЭС Дэвис-Бесс была полностью обесточена. Причина – невозможность использования автоматической системы мониторинга безопасности из-за поражения вирусом («червем») Slammer
Отключение АЭС Хатч, США	Март, 2008	Аварийное отключение АЭС Хатч (штат Джорджиа) по причине невозможности обновления программного обеспечения, установленного на единственном компьютере диспетчера
«Червь» Stuxnet	Июль, 2010	«Червь» Stuxnet, разработанный специально для поражения установок для обогащения урана в Иране. Распространялся по компьютерам сторонних пользователей, не оказывая деструктивного воздействия
Блэкаут в Венесуэле	Март, 2019	Предположительно, кибератака на систему автоматического контроля ГЭС «Эль Гури» (по заявлениям правительства Венесуэлы) привела к отключению оборудования ГЭС и прекращению электроснабжения почти 80 % потребителей страны [9]
Хакерская атака на очистные сооружения в штате Флорида, США	Февраль, 2021	Атака по каналам передачи информации привела к получению возможности удаленного управления информационной системой очистных сооружений и станций водоподготовки в штате. Целью воздействия было увеличение введения гидроксида натрия (едкий натр, NaOH) до опасного уровня
Атака через программное обеспечение компании SolarWinds, США	Декабрь, 2020	Вирус, содержавшийся в обновлении программного обеспечения компании SolarWinds, позволил получить функции удаленного администрирования применительно к тысячам телекоммуникационных сетей. Жертвами атаки стали Министерство финансов США, Национальное управление по телекоммуникациям и информации, Министерство торговли США, Министерство внутренней безопасности, отдельные компании энергетического сектора в США и Европе

Окончание таблицы

1	2	3
Атака на сетевые объекты критической инфраструктуры Дании	Май, 2023	В результате воздействия многие сети передачи данных оказались отключены от интернета, что ограничило возможность передачи диспетчерской информации в единую энергосистему страны
Похищение данных у компании Schneider Electric	Январь и ноябрь, 2024	Система организации взаимодействия с пользователями и управление корпоративной системой хранения информации были скомпрометированы. В результате взлома были украдены данные проектов и личные данные пользователей
Взлом системы управления плотиной Rizevatnet, Норвегия	Апрель, 2025	Демонстрация уязвимости системы управления по причине простого пароля. Ущерб нанесен не был (спуск воды был увеличен только на 5 %)

Очень часто незамеченным остается вмешательство, направленное исключительно на сбор информации. Например, в контексте атак на конфиденциальность, нацеленных на получение данных об использовании электроэнергии, следует отметить «интеллектуальные» счетчики, установленные у потребителей и являющиеся воплощением концепции IoT (англ. Internet of Things, интернет вещей). Данные счетчики собирают подробную информацию о потреблении электроэнергии несколько раз в час, потенциально раскрывая конфиденциальную информацию, такую как ежедневный распорядок жизни домовладельцев [10, 11]. Знание о режиме присутствия позволяет повысить успешность квартирных краж. Обнаружение утечки данных из схем использования имеет решающее значение в этом сценарии. Предназначенные в первую очередь для уменьшения хищений энергии за счет усовершенствованных алгоритмов выявления аномалий в электропотреблении, многие из «умных» счетчиков, по причине несовершенства программного обеспечения или заведомого упрощения микропроцессорной составляющей для удешевления производства, имеют чрезвычайно низкий уровень защищенности. В связи с этим получение данных со счетчиков, а также возможное перепрограммирование измерительного устройства, направленное на искажение результатов, потенциально реализуемо при незначительных временных затратах с использованием доступных информационных средств. С учетом того, что, как правило, никаких средств, ограничивающих попытки подключения, в «умные» счетчики не встроено, наиболее простой и одновременно выгодной является атака перебором (brute-force).

Отдельно стоит отметить наличие уязвимостей, связанных с наличием сервисных кодов и режимов доступа, предназначенных для первоначальной настройки, а также обслуживания измерительного комплекса в рамках проверки работоспособности и поверки прибора. Доступность размещения информации в интернете привела к тому, что сведения об указанных кодах становятся общеизвестными в течение непродолжительного времени,

приводя к массовому использованию указанной бреши в защищенности функционирования системы учета. В силу универсальности кода, записанного в микропроцессоре измерительного устройства, для нескольких сходных устройств (моделей счетчика) может быть использован общий код доступа.

В мире растет интерес со стороны ресурсоснабжающих компаний к централизованному сбору показаний систем учета. В связи с ограниченной возможностью по прокладке дополнительных линий коммуникаций между средствами учета и системой сбора и обработки информации предпочтение отдается системам беспроводной передачи информации (в радиодиапазонах сотовой связи – для большого радиуса передачи или посредством Wi-Fi для малого), а также системам передачи сигнала непосредственно по электрическим линиям (Power-line communication, PLC). Недостатком обоих указанных видов коммуникации с точки зрения безопасности является использование широковещательных технологий передачи сигнала, что позволяет, при некоторых условиях, осуществлять скрытый перехват информации, а также оказывать воздействие, направленное на создание помех, ограничивающих ее передачу.

В отличие от других видов коммуникаций, передача информации в сетях энергетических компаний менее подвержена атакам, совершаемым при помощи методов социальной инженерии. Это связано с тем, что основными участниками обмена информацией выступают информационные системы с минимальным участием человека. Тем не менее увеличение функциональности таких устройств за счет добавления интерпретаторов языков (например, Python) приводит к появлению возможности стороннего нелегитимного воздействия на работу за счет подмены компонента системы в результате целенаправленного воздействия на репозиторий хранения исходного кода [12]. С учетом роста количества задействованных программных средств, а также децентрализованного подхода к их разработке увеличивается количество потенциальных путей вмешательства в программный механизм работы многих современных средств, применяемых в энергетике [13].

Отдельно стоит отметить участившиеся случаи интеграции сторонних неавторизированных элементов в системы сбора и обработки телеметрической информации, что вызвано желанием части потребителей уменьшить величину платежей за электрическую энергию, а также стремлением некоторых государств иметь доступ к критической инфраструктуре страны-конкурента [14]. Как правило, это связано с тем, что массовое производство электронных компонентов, особенно с использованием современных технологических процессов, сосредоточено в странах Юго-Восточной Азии. Страны-заказчики определяют только общие технические требования к изделию и намного реже являются разработчиками принципиальных схем. По этой причине факт наличия нелегитимных компонентов может долго оставаться невыявленным, что увеличивает как риски воздействия со стороны разработчика указанного устройства (или непосредственного заказчика данного воздействия), так и со стороны других субъектов, получивших доступ к информации о наличии определенной уязвимости. В данном случае наличие уязвимости, заложенной непосредственно в схемотехнику электронного компонента, делает ее устранение практически невозможным.

Статистика атак, учитывающая невзаимоисключающие факторы, отмечает рост числа атак на топливно-энергетический комплекс Российской Федерации на 40 % за

первое полугодие 2025 года [15]: Из них 67 % атак начинаются с фишинговых писем, направленных на получение доступа к информационной инфраструктуре предприятия;

41 % атак направлены на промышленный шпионаж с целью получения данных исследований и перспективных разработок для последующей их перепродажи или использования инсайдерской информации на рынке ценных бумаг;

25 % нацелены на финансовые данные для получения прибыли на рынке акций;

17 % совершаются хакерами и носят деструктивный характер, направленный на достижение определенных политических или социальных целей;

17 % имеют смешанную мотивацию.

Большая часть технических мероприятий, направленных на злонамеренное воздействие на электрические сети, может быть отнесена к одному из указанных ниже типов:

1. Атака с внедрением данных в энергосистемы, известная также как манипуляция данными. Это тип кибератаки, заключающийся во внедрении ложных или вредоносных данных в системы управления энергосистемой. Целью данных атак является нарушение нормальной работы энергосистемы и потенциальное повреждение системы. Такие атаки могут принимать различные формы, но обычно они заключаются в том, что злоумышленник внедряет ложные или вредоносные данные в системы управления энергосистемой, чтобы ввести операторов в заблуждение или вызвать сбой в работе системы. Например, злоумышленник может внедрить ложные данные о неисправности в элементе энергосистемы. При ограниченных возможностях контроля и мониторинга оперативно-диспетчерский персонал предпримет действия, направленные на устранение неисправности, а также на предотвращение возможного негативного развития ситуации, вызванной отказом. В этом случае часть энергосистемы может быть выведена из эксплуатации. Атаки с внедрением данных обнаружить сложно, поскольку они часто подразумевают вброс небольшого количества ложных данных в системы управления энергосистемой. Их также сложно предотвратить, поскольку это требует высокого уровня доступа к системам управления энергосистемой. Операторам энергосистем необходимо внедрять надежные меры контроля и резервирования передачи информации для защиты от подобных атак.

2. Атака с изменением настроек релейной защиты в энергосистемах. Это специфический тип кибератаки, включающий изменение уставок срабатывания различных защитных реле – электрических и электронных устройств, которые используются для автоматического обнаружения и реагирования на аномальные состояния в энергосистеме, такие как короткие замыкания, перегрузка, отключение напряжения. Защитные реле являются важным компонентом системы защиты энергосистемы, поскольку помогают обеспечить стабильность и надежность работы сети. При атаке с изменением настроек реле злоумышленник может попытаться манипулировать их настройками, чтобы нарушить нормальную работу энергосистемы. Например, он может изменить настройки реле таким образом, чтобы они не реагировали на определенные типы неисправностей или реагировали несоответствующим образом. Это может привести к масштабным отключениям электроэнергии и другим сбоям в энергосистеме. Атаки с изменением настроек реле сложно обнаружить, так как в современных системах возможность изменения уставок заложена в концепцию SMART GRID, направленную на повышение степени автоматизации, а также на регулирование режимов с минимальным воздействием

человека. В современных микропроцессорных реле настройка уставок производится после их расчета на основании данных о режиме. Даже небольшое изменение кратности тока срабатывания может привести к отключению при токах перегрузки вместо тока однофазного короткого замыкания.

3. Атака с передачей команд на отключение. При таком типе атаки управляемый орган (реле, контактор) размыкает цепь командой, полученной из удаленного местоположения. Целью в данном случае является отключение силового коммутационного оборудования, что может привести к лавинообразным масштабным отключениям электроэнергии и другим сбоям в энергосистеме. Атаки достаточно сложно выявить, так как, как правило, подобные команды управления шифруются недостаточно эффективно и потому легко могут быть воспроизведены злоумышленниками.

Таким образом, унификация обмена данными в системах передачи критической информации, построенная вокруг поддержки протоколов наименее защищенных компонентов (поддерживающих только слабые виды шифрования в силу невысокой вычислительной мощности) негативно сказывается на общей информационной защищенности энергосистемы. Ограничение поставок электронных компонентов, вызванное санкционным давлением на РФ в 2022–2025 годах, а также отсутствие или ограниченная представленность на рынке этих компонентов российского производства приводят к вынужденному снижению темпов внедрения «цифровых подстанций».

Анализ публикаций [16–18] показывает, что тема защиты от неавторизованного и деструктивного воздействия на энергетические коммуникации регулярно поднимается авторитетными организациями, однако, в силу гетерогенности всего информационного пространства систем управления энергетикой (в первую очередь – ее электроэнергетической составляющей), вопрос может быть решен только в рамках разработки унифицированных международных стандартов, в которых основными приоритетами станут именно надежность и безопасность. Некоторые подвижки в этой области позволяют надеяться на то, что в ближайшие годы при планировании строительства новых и модернизации существующих систем управления в энергетике предпочтения по выбору технических решений сместятся в сторону высоконадежных (во всех отношениях) решений. Открытость архитектуры и соответствие стандартам позволят добиться снижения рисков негативных последствий по причине доступности аудита для выявления возможных непреднамеренных, а также специально внедренных уязвимостей. В силу отсутствия необходимости в чрезвычайно развитых технологических процессах для производства подобных электронных компонентов выпуск подобных микропроцессоров может быть налажен и на базе технологий, имеющихся в доступе у многих стран (технологические нормы проектирования – от 65 до 130 нм), включая технологические мощности Российской Федерации.

СПИСОК ЛИТЕРАТУРЫ

1. Sorebo G.N., Echols M.C. Smart Grid Security: An End-to-End View of Security in the New Electrical Grid. New York: Taylor & Francis, 2011.
2. Wang W., Lu Zh. Cyber security in the Smart Grid: Survey and challenges // *Computer Networks.* № 57. P.1344–1371. DOI:10.1016/j.comnet.2012.12.017
3. Киберугрозы и кибербезопасность в электроэнергетических системах / Н.И. Воропай [и др.]. *Электроэнергетика глазами молодежи – 2019: Материалы юбилейной*

X Международной научно-технической конференции, Иркутск, 16–20 сентября 2019 года. Иркутск: Иркутский национальный исследовательский технический университет, 2019. Т. 1. С. 32–37.
4. Белоус А.И. Кибербезопасность объектов топливно-энергетического комплекса. Концепции, методы и средства обеспечения. Вологда: Инфра-Инженерия, 2020. 644 с.
5. Мамонова Е. Сектор энергетики стал одной из основных мишеней кибератак // *Российская газета*. 2022. № 105 (8753). С.4.
6. Осак А.Б., Панасецкий Д.А., Бузина Е.Я. Кибербезопасность объектов электроэнергетики как фактор надежности ЭЭС. *Методические вопросы исследования надежности больших систем энергетики: Сборник научных статей. Вып. 66. Актуальные проблемы надежности систем энергетики*. Минск: БНТУ, 2015. DOI:10.13140/RG.2.1.2557.7849.
7. Ярушевский Д. Кибербезопасность объектов электроэнергетики: вчера, сегодня, завтра // *Безопасность объектов ТЭК*. 2017. Т. 1. С. 98–101.
8. Potential Smart Grid Vulnerabilities to Cyber Attacks: Current Threats and Existing Mitigation Strategies / Bishowjit Paul [et al.] // *Heliyon*. Vol. 10. Iss.19. 2024. URL: https://doi.org/10.1016/j.heliyon.2024.e37980 (дата обращения: 19.11.2025).
9. Новиков С. Почему произошла авария на ГЭС в Венесуэле // *Российская газета*. 2019. 10 марта. № 52 (7810). С. 2.
10. Attacks, Vulnerabilities and Security Requirements in Smart Metering Networks // *KSII Transactions on Internet and Information Systems*. Vol. 9. No. 4. Korean Society for Internet Information (KSII), 30 Apr. 2015. DOI:10.3837/tiis.2015.04.013.
11. Silva J.F.R. da. A Fast Attack against a Smart Meter Authentication Protocol. URL: https://doi.org/10.7763/IPCBEE (дата обращения: 19.01.2026).
12. Сурабекянц С. Миллионы компьютеров оказались под угрозой взлома из-за критической уязвимости, связанной с Python // *3Dnews*. 2025. 10 марта. URL: https://3dnews.ru/1119504/millioni-kompyuterov-okazalis-pod-ugrozoy-vzloma-izza-kriticheskoy-uyazvimosti-svyazannoy-s-python (дата обращения: 19.11.2025).
13. Podkuiko D. Vulnerabilities in Advanced Metering Infrastructure. Master of Science degree thesis (Computer Science and Engineering). USA. The Pennsylvania State University. 2012. 55 p. URL: https://etda.libraries.psu.edu/files/final_submissions/1591 (дата обращения: 19.11.2025).
14. Kenn J.K. Cybersecurity in Electrical Power Systems Engineering: A Practical Guide and Applications to Protecting Smart Grids, SCADA, and Critical Power Infrastructure from Cyber Attacks (Kindle Edition). Amazon. 2025. 122 p.
15. Вяткина А., Осипова А. Актуальные киберугрозы: I–II кварталы 2025 года // *Positive Technologies*. 28 августа 2025. URL: https://ptsecurity.com/research/analytics/aktual-nye-kiberugrozy-i-ii-kvartaly-2025-goda/ (дата обращения: 19.11.2025).
16. Kreso I. Cyber Threats and Vulnerability Mapping in the Energy Sector: Laying the Groundwork for smart Grid Resilience // *ACIG*. Vol. 4. No. 1, 2025. DOI: 10.60097/ACIG/211124.
17. Critical Infrastructure Annual Risk Review. Third Edition. November 2025. Australian Government. Department of Home Affairs. Critical infrastructure security centre. URL: https://www.cisc.gov.au/resources-subsite/Documents/critical-infrastructure-annual-risk-review-2025.pdf (дата обращения: 19.11.2025).

18. IEA (2025). World Energy Outlook 2025. IEA. Paris. URL: https://www.iea.org/reports /world-energy-outlook-2025 (дата обращения: 19.11.2025).

СВЕДЕНИЯ ОБ АВТОРАХ

КОРНЕЕВ Константин Борисович – кандидат технических наук, доцент кафедры электроснабжения и электротехники, ФГБОУ ВО «Тверской государственный технический университет», 170026, Россия, г. Тверь, наб. А. Никитина, д. 22. E-mail: Energy-tver@mail.ru
КОРНЕЕВ Виктор Константинович – студент, ФГАОУ ВО «Национальный исследовательский технологический университет «МИСИС», 119049, Россия, Москва, Ленинский пр-кт, д. 4, стр. 1. E-mail: korneyev.viktor@mail.ru

БИБЛИОГРАФИЧЕСКАЯ ССЫЛКА

Корнеев К.Б., Корнеев В.К. Обеспечение информационной безопасности в электроэнергетике // Вестник Тверского государственного технического университета. Серия «Строительство. Электротехника и химические технологии». 2026. № 1 (29). С. 50–58.

ENSURING INFORMATION SECURITY IN THE ELECTRIC POWER INDUSTRY

Korneev K.B.[1], Korneev V.K.[2]
[1] Tver State Technical University (Tver),
[2] University of Science and Technology «MISIS» (Moscow)

Abstract. The increasing use of information technology in the industrial sector, and most importantly in such critical area as energy production, necessitates the development of systems to control the flow of information collected, transmitted, and processed at power enterprises. While transferring information storage and processing to the “cloud” improves reliability and processing speed, it also makes the system more vulnerable to illegitimate external influence. The integration of highly connected Internet of Things (IoT) network elements can also negatively impact information security.

Keywords: Electric power industry, information security, cyberattack, cybercrime, reliability.

INFORMATION ABOUT THE AUTHORS

KORNEEV Konstantin Borisovich – Candidate of Technical Sciences, Associate Professor of the Department of Power Supply and Electrical Engineering, Tver State Technical University, 22, embankment of A. Nikitin, Tver, 170026, Russia. E-mail: Energy-tver@mail.ru
KORNEEV Viktor Konstantinovich – student, Federal State Educational Institution of Higher Education «National Research Technological University «MISIS», 4, Leninsky Prospekt, building 1, Moscow, 119049, Russia. E-mail: korneyev.viktor@mail.ru

CITATION FOR AN ARTICLE

Korneev K.B., Korneev V.K. Ensuring information security in the electric power industry// Vestnik of Tver State Technical University. Series «Building. Electrical engineering and chemical technology». 2026. No. 1 (29), pp. 50–58.